

EXHIBIT 7

1 PIERCE O'DONNELL (SBN 081298)
2 PODonnell@GreenbergGlusker.com
3 TIMOTHY J. TOOHEY (SBN 140117)
4 TToohey@GreenbergGlusker.com
5 PAUL BLECHNER (SBN159514)
6 PBlechner@GreenbergGlusker.com
7 GREENBERG GLUSKER FIELDS CLAMAN &
8 MACHTINGER LLP
9 1900 Avenue of the Stars, 21st Floor
10 Los Angeles, California 90067-4590
11 Telephone: 310.553.3610
12 Fax: 310.553.0687

13
14 Attorneys for Plaintiff
15 **MICHAEL TERPIN**

16 UNITED STATES DISTRICT COURT
17 CENTRAL DISTRICT OF CALIFORNIA

18 MICHAEL TERPIN,
19
20 Plaintiff,
21
22 v.
23 AT&T INC.; AT&T Mobility, LLC;
24 and DOES 1-25,
25
26 Defendants.

Case No. 2:18-cv-6975

COMPLAINT FOR:

(1) **DECLARATORY RELIEF: UNENFORCEABILITY OF AT&T CONSUMER AGREEMENT AS UNCONSCIONABLE AND CONTRARY TO PUBLIC POLICY;**
(2) **UNAUTHORIZED DISCLOSURE OF CUSTOMER CONFIDENTIAL PROPRIETARY INFORMATION AND PROPRIETARY NETWORK INFORMATION, FEDERAL COMMUNICATIONS ACT, 47 U.S.C. §§ 206, 222;** (3) **ASSISTING UNLAWFUL ACCESS TO COMPUTER, CAL. PENAL CODE § 502 ET SEQ.;** (4) **VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW—UNLAWFUL BUSINESS PRACTICE CAL. BUS. & PROF. CODE § 17200 ET SEQ.;** (5) **VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW—UNFAIR BUSINESS PRACTICE,**

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

CAL. BUS. & PROF. CODE § 17200 ET SEQ.; (6) VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW—FRAUDULENT BUSINESS PRACTICE CAL. BUS. & PROF. CODE § 17200 ET SEQ.; (7) VIOLATION OF CALIFORNIA CONSUMER LEGAL REMEDIES ACT, CAL. CIV. CODE § 1750 ET SEQ.; (8) DECEIT BY CONCEALMENT, CAL. CIV. CODE §§ 1709, 1710; (9) MISREPRESENTATION; (10) NEGLIGENCE; (11) NEGLIGENT SUPERVISION AND TRAINING; (12) NEGLIGENT HIRING; (13) BREACH OF CONTRACT—AT&T PRIVACY POLICY; (14) BREACH OF IMPLIED CONTRACT IN THE ALTERNATIVE TO BREACH OF CONTRACT; (15) BREACH OF COVENANT OF GOOD FAITH AND FAIR DEALING; (16) VIOLATION OF CALIFORNIA CONSUMER RECORDS ACT—INADEQUATE SECURITY, CAL. CIV. CODE § 1798.81.5

DEMAND FOR JURY TRIAL

Plaintiff Michael Terpin, by and through his counsel, complains and alleges as follows against AT&T, Inc. and its wholly owned subsidiary AT&T Mobility, LLC (collectively, “AT&T”):

JURISDICTION AND VENUE

1. This Court has jurisdiction over this matter under 28 U.S.C. § 1331 because this case arises under federal question jurisdiction under the Federal Communications Act (“FCA”). The Court has supplemental jurisdiction under 28 U.S.C. § 1367 over the state law claims because the claims are derived from a common nucleus of operative facts. The Court also has jurisdiction over this matter under 28 U.S.C. § 1332 in that the amount in controversy exceeds \$75,000 and Plaintiff and Defendants are citizens of different states in that Plaintiff, Michael Terpin is domiciled in Puerto Rico with a residence in California, and Defendants

1 AT&T, Inc. and AT&T Mobility, Inc., are corporations with their principal places
2 of business, respectively, in Texas and Georgia.

3 2. Venue is proper in this Court under 28 U.S.C. §§ 1391(b)(1),
4 (b)(2), (c) and (d) because a substantial part of the events or omissions giving rise
5 to this Complaint occurred in this District. Plaintiff Michael Terpin has a residence
6 in Los Angeles County, California. Mr. Terpin obtained wireless services from
7 AT&T in Los Angeles County in or about the mid-1990's. AT&T does business in
8 and is subject to the Court's jurisdiction in this District. AT&T's violation of Mr.
9 Terpin's privacy in those services is the subject of this complaint. Mr. Terpin
10 continued at all times relevant to the allegations herein to receive wireless services
11 from AT&T for a telephone number with a Southern Californian area code.

12 INTRODUCTION

13 3. AT&T solemnly promises its cellular telephone subscribers that
14 it will safeguard their private information—and particularly their data-rich SIM
15 cards—from any unauthorized disclosure. Besides the numerous promises that
16 AT&T makes in its own Privacy Policy and Code of Business Conduct, federal and
17 state law impose a strict duty on the nation's second largest cellular telephone
18 carrier to take all necessary steps to preserve the privacy of its almost 140 million
19 customers. In AT&T's case, this mandate has fallen on deaf ears.

20 4. In one notorious instance, AT&T employees were found
21 culpable for stealing personal information for over 200,000 customers and selling it
22 to criminals to unlock mobile phones. This massive security failure prompted the
23 Federal Communications Commission to levy a record fine of \$25 million and
24 secure a Consent Decree requiring AT&T to implement detailed measures to
25 enhance its subscribers' protection against unauthorized disclosures of their private
26 information. AT&T did not learn its lesson.

27 5. More recently, AT&T employees are participating in a new
28 species of fraud—SIM swap fraud—which is a metastasizing cancer attacking

1 AT&T customers and allowing hackers readily to bypass AT&T security to rob
2 AT&T customers of valuable personal information and millions of dollars of
3 cryptocurrency.

4 6. AT&T's subscriber privacy protection system is thus a veritable
5 modern-day Maginot Line: a lot of reassuring words that promote a false sense of
6 security. AT&T persists in not providing adequate security even though it knows
7 that hackers target its systems because the hackers know they are riddled with
8 flaws. Most troubling, AT&T has not improved its protections even though it
9 knows from numerous incidents that some of its employees actively cooperate with
10 hackers in SIM swap frauds by giving hackers direct access to customer
11 information and by overriding AT&T's security procedures. In recent incidents,
12 law enforcement has even confirmed that AT&T employees profited from working
13 directly with cyber terrorists and thieves in SIM swap frauds.

14 7. The porosity of AT&T's privacy program is dramatically
15 evident in this case, which follows a pattern well known to AT&T. An
16 experienced, high profile cryptocurrency investor, Plaintiff Michael Terpin was a
17 longtime AT&T subscriber who entrusted his sensitive private information to
18 AT&T and relied on AT&T's assurances and its compliance with applicable laws.
19 Given all the carrier's hype about protecting customer security, Plaintiff believed
20 that it would keep its promises about absolutely safeguarding him from a data
21 breach that could lead to the theft of tens of millions of dollars of crypto currency.
22 In reality, however, Plaintiff was victimized by not one, but two hacks within seven
23 months.

24 8. Even after AT&T had placed vaunted additional protection on
25 his account after an earlier hacking incident, an imposter posing as Mr. Terpin was
26 able to easily obtain Mr. Terpin's telephone number from an insider cooperating
27 with the hacker without the AT&T store employee requiring him to present valid
28 identification or to give Mr. Terpin's required password.

1 9. The purloined telephone number was accessed to hack Mr.
2 Terpin's accounts, resulting in the loss of nearly \$24 million of cryptocurrency
3 coins.

4 10. It was AT&T's act of providing hackers with access to Mr.
5 Terpin's telephone number without adhering to its security procedures that allowed
6 the cryptocurrency theft to occur. What AT&T did was like a hotel giving a thief
7 with a fake ID a room key *and* a key to the room safe to steal jewelry in the safe
8 from the rightful owner.

9 11. AT&T is doing nothing to protect its almost 140 million
10 customers from SIM card fraud. AT&T is therefore directly culpable for these
11 attacks because it is well aware that its customers are subject to SIM swap fraud
12 and that its security measures are ineffective. AT&T does virtually nothing to
13 protect its customers from such fraud because it has become too big to care.

14 12. This lawsuit seeks to hold AT&T accountable for its abject
15 failure to protect subscribers like Mr. Terpin. Apparently, AT&T would prefer to
16 buy Time Warner for over \$85 billion than pay for a state-of-the art security system
17 and hire, train, and supervise competent and ethical employees—even when it was
18 well known to AT&T that its system was vulnerable to precisely the type of hack
19 experienced by Mr. Terpin. A verdict for \$24 million of compensatory damages
20 and over \$200 million for punitive damages might attract the attention of AT&T's
21 senior management long enough to spend serious money on an acceptable customer
22 protection program and measures to ensure that its own employees are not
23 complicit in theft and fraud. Then and only then will AT&T's promise to protect
24 the types of personal information that directly led to the hacking of Mr. Terpin's
25 accounts ring true.

THE PARTIES

13. Mr. Terpin is well known for his involvement with cryptocurrency. Cryptocurrency (also known as “crypto”) is digital or virtual currency designed as a medium of exchange in which encryption techniques generate units of currency that verify the transfer of funds through an encrypted ledger called “blockchain.” Cryptocurrency is decentralized, operates independently of a central bank, and is often traded by parties through “exchanges.” The total market value of all cryptocurrency has previously exceeded \$800 billion, and there are many who project it to hit \$1 trillion by the end of 2018.

14. Mr. Terpin is a prominent member of the blockchain and cryptocurrency community. In 2013, he started Bit Angels, the first angel group for investing in bitcoin companies, and CoinAgenda, the first high-end investor series for family offices and funds investing in digital assets. Mr. Terpin also runs the preeminent public relations firm in the cryptocurrency sector. Like others in the cryptocurrency community, Mr. Terpin is a high-profile hacker target because of his publicized involvement in cryptocurrency enterprises.

15. AT&T, Inc. is a Delaware Corporation with its principal place of business in Dallas, Texas. AT&T Mobility, LLC (“AT&T Mobility”), which is marketed as “AT&T,” is a wholly-owned subsidiary of AT&T, Inc. with its principal place of business in Brookhaven, Georgia. AT&T Mobility provides wireless service to subscribers in the United States, Puerto Rico, and the U.S. Virgin Islands. AT&T Mobility is a “common carrier” governed by the Federal Communications Act (“FCA”), 47 U.S.C. § 151 *et seq.* AT&T Mobility is regulated by the Federal Communications Commission (“FCC”) for its acts and practices, including those occurring in this District. AT&T, Inc. and AT&T Mobility are herein referred to collectively as “AT&T.”

16. AT&T Mobility is the second largest wireless provider in the United States with 138.8 million subscribers as of the third quarter of 2017. AT&T, Inc., as it is presently constituted, is the result of the recombination of many of the companies split off from the original AT&T (also known as “The Telephone Company” or “Ma Bell.”) AT&T, Inc. is a behemoth which, in 2017, had operating revenues of over \$160 billion and assets of over \$444 billion.

17. Over the past decade, AT&T has gone on a buying spree costing over \$150 billion, acquiring: Bell South (including Cingular Wireless and Yellowpages.com), Dobson Communications, Edge Wireless, Cellular One, Centennial, Wayport, Qualcomm Spectrum, Leap Wireless, DirecTV, and Iusacell and NII Holdings (now AT&T Mexico). During the same period, AT&T’s mobile phone business was rated as the worst among major providers. *Consumer Reports* named it the “worst carrier” in 2010, and the next year, J.D. Power found AT&T’s network the least reliable in the country—a dubious achievement that it also earned in prior years. Little wonder that its customers were the least happy of subscribers of the Big Four carriers according to the American Consumer Index. In the meantime, AT&T has purchased for a total equity value of \$85.4 billion Time Warner Inc.—the owner of HBO, Warner Bros, CNN, Turner Broadcasting, Cartoon Network, Turner Classic Movies, TBS, TNT and Turner Sports.

18. According to media reports, AT&T mobile telephone customers have been the subject of more privacy violations than subscribers to other cell phone companies. The Electronic Frontier Foundation has recently called out AT&T’s “hypocrisy” in calling for an “Internet Bill of Rights” when in fact “few companies have done more to combat privacy and network neutrality than AT&T.” <https://www.eff.org/deeplinks/2018/01/hypocrisy-atts-internet-bill-rights> AT&T has even lobbied the FCC to stop applying the privacy provisions of the FCA to its broadband services, while arguing (unsuccessfully) that it was not subject to the jurisdiction of the Federal Trade Commission (“FTC”) to govern privacy and data

1 security pursuant to its jurisdiction to regulate unfair and deceptive acts under
2 Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1)(2).

3 19. As further detailed below, AT&T has also been subject to other
4 incidents of SIM card swap fraud, including incidents involving prominent
5 members of the cryptocurrency community. It is further aware that its employees
6 are complicit in such fraud and can bypass AT&T's security concerns. Despite the
7 incidents, AT&T persists in not securing its system against a cresting wave of such
8 fraudulent activity.

9 20. Given AT&T's dismal track record on consumer privacy,
10 including the FCC's fine and Consent Decree referenced below and its failure to
11 prevent fraud of the sort that victimized Mr. Terpin, it ought to invest its money and
12 attention to protecting its cellular telephone subscribers from the onslaught of
13 hacking and insider data breaches before it spends billions of dollars for new
14 companies, like Time Warner. After all, AT&T was historically a *telephone*
15 company.

16 21. Plaintiff is ignorant of the true names or capacities of the
17 defendants sued herein under the fictitious names DOES ONE through TWENTY-
18 FIVE inclusive. Plaintiff further alleges that each of the fictitiously named
19 Defendants is responsible in some manner for the occurrences herein alleged,
20 proximately caused plaintiff's damages, and was acting as agent for the others.

21 **FACTUAL ALLEGATIONS**

22 **AT&T'S STATUTORY OBLIGATION TO PROTECT** 23 **CUSTOMERS' PERSONAL INFORMATION** 24 **UNDER THE FEDERAL COMMUNICATIONS ACT**

25 22. As a common carrier, AT&T is obligated to protect the
26 confidential personal information of its customers under Section 222 of the FCA,
27 47 U.S.C. § 222.
28

1 23. Section 222(a), 47 U.S.C. § 222(a), provides that “[e]very
2 telecommunications carrier has a duty to protect the confidentiality of proprietary
3 information of, and relating to . . . customers . . .” The “confidential proprietary
4 information” referred to in Section 222(a), is abbreviated herein as “CPI.”

5 24. Section 222(c), 47 U.S.C. § 222(c), additionally provides that
6 “[e]xcept as required by law or with the approval of the customer, a
7 telecommunications carrier that receives or obtains customer proprietary network
8 information by virtue of its provision of a telecommunications service shall only
9 use, disclose, or permit access to individually identifiable customer proprietary
10 network information in its provision of (A) the telecommunications service from
11 which such information is derived, or (B) services necessary to, or used in, the
12 provision of such telecommunications service, including the publishing of
13 directories.” The “customer proprietary network information” referred to in
14 Section 222(c) is abbreviated herein as “CPNI.”

15 25. Section 222(h)(1), 47 U.S.C. § 222(h)(1), defines CPNI as
16 “(A) information that relates to the quantity, technical configuration, type,
17 destination, location, and amount of use of a telecommunications service subscribed
18 to by any customer of a telecommunications carrier, and that is made available to
19 the carrier by the customer solely by virtue of the carrier-customer relationship; and
20 (B) information contained in the bills pertaining to telephone exchange service or
21 telephone toll service received by a customer of a carrier, except that term does not
22 include subscriber list information.”

23 26. The FCC has promulgated rules to implement Section 222 “to
24 ensure that telecommunications carriers establish effective safeguards to protect
25 against unauthorized use or disclosure of CPNI.” *See* 47 CFR § 64.2001 *et seq.*
26 (“CPNI Rules”); *CPNI Order*, 13 FCC Rcd. at 8195 ¶ 193. The CPNI Rules limit
27 disclosure and use of CPNI without customer approval to certain limited
28

1 circumstances (such as cooperation with law enforcement), none of which are
2 applicable to the facts here. 47 CFR § 64.2005.

3 27. The CPNI Rules require carriers to implement safeguards to
4 protect customers' CPNI. These safeguards include: (i) training personnel "as to
5 when they are and are not authorized to use CPNI"; (ii) establishing "a supervisory
6 review process regarding carrier compliance with the rules;" and (iii) filing annual
7 compliance certificates with the FCC. 47 CFR § 64.2009(b), (d), and (e).

8 28. The CPNI Rules further require carriers to implement measures
9 to prevent the disclosure of CPNI to unauthorized individuals. 47 CFR § 64.2010.
10 For example, "carriers must take reasonable measures to discover and protect
11 against attempts to gain unauthorized access to CPNI." 47 CFR § 64.2010(a).
12 Moreover, "carriers must properly authenticate a customer prior to disclosing CPNI
13 based on customer-initiated telephone contact, online account access, or an in-store
14 visit." *Id.* In the case of in-store access to CPNI, "[a] telecommunications carrier
15 may disclose CPNI to a customer who, at a carrier's retail location, *first presents to*
16 *the telecommunications carrier or its agent a valid photo ID matching the*
17 *customer's account information.*" 47 CFR § 64.2010(d) (emphasis added). "Valid
18 photo ID" is defined in 47 CFR § 64.2003(r) as "a government-issued means of
19 personal identification with a photograph such as a driver's license, passport, or
20 comparable ID that is not expired."

21 29. The FCC has determined that information obtained from
22 customers through a common social engineering ploy known as "pretexting" is
23 CPNI. *See In the Matter of Implementation of the Telecommunications Acts of*
24 *1996: Telecommunications Carriers' Use of Customer Proprietary Network*
25 *Information and Other Customer Information*, 22 FCC Rcd. 6927 (2007)
26 ("Pretexting Order"). Pretexting is "the practice of pretending to be a particular
27 customer or other authorized person in order to obtain access to that customer's call
28 detail or other private communications records." *Id.*, n. 1. Such "call detail" and

1 “private communications” are CPI and CPNI under the FCA. *Id.* at 6928 *et seq.*
2 The FCC concluded that “pretexters have been successful at gaining unauthorized
3 access to CPNI” and that “carriers’ record on protecting CPNI demonstrate[d] that
4 the Commission must take additional steps to protect customers from carriers that
5 have failed to adequately protect CPNI.” *Id.* at 6933. The FCC modified its rules to
6 impose additional security for carriers’ disclosure of CPNI and to require that law
7 enforcement and customers be notified of security breaches involving CPNI. *Id.* at
8 6936-62.

9 30. In its Pretexting Order, the FCC stated that it “fully expect[s]
10 carriers to take every reasonable precaution to protect the confidentiality of
11 proprietary or personal customer information.” *Id.* at 6959, ¶ 64. The FCC further
12 stated that “[w]e decline to immunize carriers from possible sanction for disclosing
13 customers’ private information without appropriate authorization.” *Id.* at 6960,
14 ¶ 66. In a statement directly relevant to the facts alleged below, the FCC also
15 stressed the fact that *someone having obtained information fraudulently is strong*
16 *evidence of the carrier’s failure to satisfy the requirements of section 222.* The
17 FCC stated that “we hereby put carriers on notice that the Commission henceforth
18 will infer from evidence that a pretexter has obtained unauthorized access to a
19 customer’s CPNI that the carrier did not sufficiently protect that customer’s CPNI.
20 A carrier then must demonstrate that the steps it has taken to protect CPNI from
21 unauthorized disclosure, including the carrier’s policies and procedures, are
22 reasonable *in light of the threat posed by pretexting and the sensitivity of the*
23 *customer information at issue.*” *Id.* at 6959, ¶ 63 (emphasis added).

24 31. As further alleged below, AT&T violated Section 222 of the
25 FCA and the CPNI Rules and ignored the warning in the Pretexting Order on
26 January 7, 2018 when its employees provided hackers with Mr. Terpin’s SIM cards
27 containing or allowing access to Mr. Terpin’s personal information, including CPI
28 and CPNI, without Mr. Terpin’s authorization or permission, and without requiring

1 that the individual accessing Mr. Terpin's account present valid identification or
2 comply with AT&T's own procedures.

3 **AT&T EMPLOYEES' DISCLOSURE OF CUSTOMERS' PERSONAL**
4 **INFORMATION AND THE APRIL 8, 2015 FCC CONSENT DECREE**

5 32. On April 8, 2015, the FCC fined AT&T a record \$25 million for
6 violating Section 222 of the FCA by allowing its employees to hand over to thieves
7 the CPNI of almost 280,000 customers. In addition to being forced to pay \$25
8 million to the FCC, AT&T entered into a consent decree requiring it to implement
9 measures to protect CPNI. The April 8, 2015 consent decree ("Consent Decree")
10 remains in full force and effect.

11 33. In the Consent Decree and the FCC's adopting order ("Adopting
12 Order"), the FCC highlights AT&T's lax security practices and dismal failure to
13 supervise and monitor employees that led to its unprecedented breach of its
14 customers' confidential and private information. *See In the Matter of AT&T*
15 *Services, Inc.*, 30 FCC Rcd. 2808 (April 8, 2015 Adopting Order and Consent
16 Decree) (attached hereto as Exhibit A).

17 34. The FCC investigation revealed that numerous AT&T call
18 center employees provided the CPNI of hundreds of thousands of customers,
19 including names, phone numbers and Social Security Numbers to unauthorized
20 third parties, who used this information to gain access to unlock codes for mobile
21 telephones and to remove territorial and network restrictions. *Id.* at 2808. The
22 investigation further revealed that employees were frequently paid by criminals to
23 hand over AT&T customers' personal sensitive information, including account-
24 related CPNI. *Id.* at 2808, 2813-15.

25 35. The FCC found that AT&T employees used their login
26 credentials to access the confidential information of almost 280,000 customers.
27 The FCC concluded that AT&T's data security measures "failed to prevent or
28 timely detect a large and ongoing Data Breach." *Id.* at 2813 (Consent Decree ¶ 8).

1 36. The FCC also found that AT&T had not properly supervised its
2 employees' access to its customers' personal information, including CPNI. The
3 FCC concluded that AT&T's "failure to reasonably secure customers' proprietary
4 information violates a carrier's statutory duty under the Communications Act to
5 protect that information and constitutes an unjust and unreasonable practice in
6 violation of the Act." *Id.* at 2808 (Adopting Order § 2).

7 37. In the Adopting Order, the FCC emphasized the importance of
8 AT&T's obligation to adhere to the obligations embodied in Section 222 of the
9 FCA. According to the Adopting Order, the purpose of Section 222 is to "ensure
10 that consumers can trust that carriers have taken appropriate steps to ensure that
11 unauthorized persons are not accessing, viewing or misusing their personal
12 information." *Id.* Carriers like AT&T are thus required to take "every reasonable
13 precaution' to protect their customers' data" and to notify consumers regarding any
14 breaches in order to "aid in the pursuit and apprehension of bad actors and provide
15 valuable information that helps affected consumers [to] be proactive in protecting
16 themselves in the aftermath of a data breach." *Id.*

17 38. As a condition of terminating the FCC's investigation of
18 AT&T's violations of Sections 201(b) and 222 of the FCA, the FCC imposed
19 numerous requirements on AT&T to improve its supervision of employees and to
20 adhere to its legal obligation to protect the privacy of AT&T's customers.
21 Moreover, the Consent Decree imposed obligations not only on AT&T itself, but
22 also on AT&T's "Covered Employees," who are defined as "all employees and
23 agents of AT&T who perform or directly supervise, oversee, or manage the
24 performance of duties that involve access to, use, or disclosure of Personal
25 Information or Customer Proprietary Network Information at Call Centers managed
26 and operated by AT&T Mobility." *Id.* at 2811. "Call Center" is defined broadly in
27 the Consent Decree as call centers operated by AT&T or its contractors "that
28

1 provide mobility customer service or wireless sale service for AT&T Mobility
2 consumer customers.” *Id.* at 2810.

3 39. Paragraph 17 of the FCC Consent Decree requires AT&T to
4 designate “a senior corporate manager with the requisite corporate and organization
5 authority to serve as a Compliance Officer . . .” *Id.* at 2816. AT&T’s Compliance
6 Officer must be “responsible for developing, implementing, and administering the
7 Compliance Plan and ensuring that AT&T complies with the terms and conditions
8 of the Compliance Plan and this Consent Decree.” *Id.*

9 40. Paragraph 18 of the FCC Consent Decree requires AT&T to
10 institute a “Compliance Plan designed to ensure future compliance with the [FCA]
11 and with the terms and conditions of this Consent Decree.” *Id.* The Compliance
12 Plan must include a Risk Assessment, Information Security Program, Ongoing
13 Monitoring and Improvement, and a Compliance Review. *Id.*

14 41. The “Information Security Program” required in
15 Paragraph 18(b) must be “reasonably designed to protect CPNI and Personal
16 Information from unauthorized access, use, or disclosure by Covered Employees . .
17 ..” *Id.* AT&T’s program must be documented in writing and include:

- 18 (i) administrative, technical, and physical safeguards reasonably
19 designed to protect the security and confidentiality of Personal
20 Information and CPNI;
- 21 (ii) reasonable measures to protect Personal Information and CPNI
22 maintained by or made available to Vendors, Covered Employees, and
23 Covered Vendor Employees. . . ;
- 24 (iii) access controls reasonably designed to limit access to Personal
25 Information and CPNI to authorized AT&T employees, agents, and
26 Covered Vendor Employees;
- 27 (iv) reasonable processes to assist AT&T in detecting and responding
28 to suspicious or anomalous account activity, including whether by

malware or otherwise, involving Covered Employees and Covered Vendor Employees; and

(v) a comprehensive breach response plan that will enable AT&T to fulfill its obligations under applicable laws, with regard to breach notifications, including its obligations under paragraph 20 while that paragraph remains in effect.

42. Paragraph 18(c) of the Consent Decree requires AT&T to “monitor its Information Security Program on an ongoing basis to ensure that it is operating in a manner reasonably calculated to control the risks identified through the Risk Assessment, to identify and respond to emerging risks or threats, and to comply with the requirements of Section 222 of the [FCA], the CPNI Rules, and this Consent Decree.” *Id.* at 2817. In addition, Paragraph 18(g) requires AT&T to “establish and implement a Compliance Training Program [for employees] on compliance with Section 222, the CPNI Rules, and the Operating Procedures.” *Id.* All “Covered Employees” are required to be trained within six months of hire and periodically thereafter. *Id.*

43. AT&T must report noncompliance with the terms and conditions of the Consent Decree within fifteen (15) days after discovery of such noncompliance. *Id.* at 2819 (Consent Decree ¶ 20). In addition, “AT&T shall also report to the FCC any breaches of Personal Information or CPNI involving any Covered Employees or Covered Vendor Employees that AT&T is required by any federal or state law to report to any Federal or state entity or any individual.” *Id.* Moreover, AT&T is required to file compliance reports with the FCC six (6) months after the Effective Date, twelve (12) months after the Effective Date, and thirty-six (36) months after the Effective Date.” *Id.* (Consent Decree ¶ 21).

44. The provisions in Paragraphs 17 and 18 of the Consent Decree were applicable at all relevant dates to the acts and omissions alleged in this Complaint. *Id.* at 2820 (Consent Decree ¶ 22 (Paragraphs 17-18 expire seven (7)

1 years after the “Effective Date,” *i.e.*, April 7, 2022)). As further alleged below,
2 AT&T violated numerous terms of the April 8, 2015 Consent Decree by failing to
3 implement adequate security procedures to protect Mr. Terpin’s personal
4 information, including CPNI, by failing to supervise and monitor its employees, by
5 failing to ensure that its employees were ethical and competent, by failing to follow
6 its security procedures and by failing to follow its legal obligations to protect Mr.
7 Terpin’s personal information under the FAC, CPNI Rules, and the Consent
8 Decree. Mr. Terpin alleges on information and belief that AT&T also failed to
9 report to the FCC the two data breaches involving Mr. Terpin, as required by FCC
10 regulations and the Consent Decree. Mr. Terpin further alleges on information and
11 belief that AT&T has failed to report to the FCC additional data breaches involving
12 victims of fraud where AT&T employees provided hackers access AT&T’s
13 customers’ telephone numbers who stole money from the customers.

14 **AT&T’S PRIVACY AND SECURITY COMMITMENTS TO CUSTOMERS**
15 **IN ITS PRIVACY POLICY AND CODE OF BUSINESS CONDUCT**

16 45. In its Privacy Policy (“Privacy Policy”) and Code of Business
17 Conduct (“COBC”), AT&T acknowledges its responsibilities to protect customers’
18 “Personal Information” under the FCA, the CPNI Rules and other regulations. A
19 true and correct copy of the Privacy Policy in effect in January 2018 available at
20 http://about.att.com/sites/privacy_policy is attached hereto as Exhibit B. A true
21 and correct copy of the COBC in effect in January 2018 available at
22 <https://ebiznet.sbc.com/attcode/index.cfm> is attached hereto as Exhibit C.

23 46. In its Privacy Policy and COBC, AT&T makes binding
24 promises and commitments to Mr. Terpin, as its customer, that it will protect and
25 secure his “Personal Information.” The Privacy Policy defines “Personal
26 Information” as “[i]nformation that identifies or reasonably can be used to figure
27 out the identity of a customer or user, such as your name, address, phone number
28 and e-mail address.” AT&T states that, among the information that it collects from

1 and about its customers, are “your name, address, telephone number, e-mail
2 address” and service-related details such as payment history, security codes, service
3 history and similar information. AT&T also collects information relating to the use
4 of its networks, products and services. “Personal Information” thus includes both
5 CPI and CPNI under Section 222 of the FCA and the CPNI Rules.

6 47. In its Privacy Policy AT&T promises that it takes its
7 responsibility “to safeguard your [*i.e.*, the customer’s] Personal Information
8 seriously” and that it will not share its customers’ Personal Information except for
9 legitimate business purposes. It further states that “we will not sell [users’]
10 Personal Information to anyone, for any purpose. Period.”

11 48. AT&T further promises that it has numerous safeguards in place
12 to protect the Personal Information of its customers and makes the following
13 promises to its customers:

14 We’ve worked hard to protect your information. *And we’ve established*
15 *electronic and administrative safeguards designed to make the information*
16 *we collect secure.* Some examples of those safeguards include:

- 17 • All of our employees are subject to the AT&T Code of Business
18 Conduct (COBC)

19 ([https://www.att.com/Common/about_us/downloads/att_code_of_busi](https://www.att.com/Common/about_us/downloads/att_code_of_business_conduct.pdf)
20 [ness_conduct.pdf](https://www.att.com/Common/about_us/downloads/att_code_of_business_conduct.pdf)) and certain state-mandated codes of conduct.

21 Under the COBC, all employees must follow the laws, rules,
22 regulations, court and/or administrative orders that apply to our
23 business—including, specifically, the legal requirements and company
24 policies surrounding the privacy of communications and the security
25 and privacy of your records. We take this seriously, and any of our
26 employees who fail to meet the standards we’ve set in the COBC are
27 subject to disciplinary action. That includes dismissal.
28

- We've implemented technology and security features and strict policy guidelines to safeguard the privacy of your Personal information. Some examples are:
 - Maintaining and protecting the security of computer storage and network equipment, and using our security procedures that require employee user names and passwords to access sensitive data;
 - Applying encryption or other appropriate security controls to protect Personal Information when stored or transmitted by us;
 - Limiting access to Personal Information to only those with jobs requiring such access; and
 - *Requiring caller/online authentication before providing Account Information so that only you or someone who knows your Account Information will be able to access or change this information.*

(Emphasis added.)

49. AT&T's COBC also makes binding commitments to Mr. Terpin, as an AT&T customer, that it will protect his Personal Information and that it will adhere to all its legal obligations. Those legal obligations include, by implication, Section 222 of the FCA, the CPNI Rules, and other legal obligations that govern protection of confidential and private information. For example, AT&T's chairman and chief executive, Randall Stephenson, and its chief compliance officer, David Huntley promise that because "[o]ur customers count on us" "[t]hat we will follow not only the letter of the law, but the spirit of the law" and "that we will always take responsibility." *The COBC also specifically promises that AT&T will "protect the privacy of our customers' communications" because "[n]ot only do our customers demand this, but the law requires it.*

1 *Maintaining the confidentiality of communication is, and always has been, a*
2 *crucial part of our business.”* (Emphasis added.)

3 50. AT&T further promises in the COBC that it “protect[s] the
4 information about our customers that they entrust to us.” Acknowledging that
5 “AT&T possesses sensitive, detailed information about our customers, who rely on
6 AT&T to safeguard that information” and that “[l]aws and regulations tell us how
7 to treat such data,” AT&T promises Mr. Terpin, as an AT&T customer, that “[a]ny
8 inappropriate use of confidential customer information violates our customers’ trust
9 and may also violate a law or regulation. *Preserving our customers’ trust by*
10 *safeguarding their private data is essential to our reputation.”* (Emphasis added.)

11 51. As alleged below, AT&T flagrantly and repeatedly violated its
12 commitments to Mr. Terpin in its Privacy Policy and COBC, as well as its legal
13 obligations under the FCA, the CPNI Rules, the Consent Decree, and California
14 law, by willingly turning over to hackers Mr. Terpin’s wireless number that allowed
15 hackers to access his “Personal Information” including CPNI. AT&T’s betrayal of
16 its obligations caused Mr. Terpin to lose nearly \$24 million worth of
17 cryptocurrency.

18 **THE PREVALENCE OF SIM CARD SWAP FRAUD**

19 52. AT&T is directly liable for the harm suffered by Mr. Terpin
20 because it has long known that its customers are subject to SIM swap fraud (also
21 called SIM swapping, SIM hijacking, or “port out scam”) perpetrated by hackers
22 often with the active cooperation of its own employees. The prevalence of such
23 fraud is established by numerous news reports, the experience of other AT&T
24 customers known to Plaintiff, and Mr. Terpin’s own doleful experience.

25 53. As described in in a July 30, 2018 article in *Motherboard*
26 entitled “‘Tell Your Dad to Give Us Bitcoin:’ How a Hacker Allegedly Stole
27 Millions by Hijacking Phone Numbers,” available at
28 https://motherboard.vice.com/en_us/article/a3q7mz/hacker-allegedly-stole-

1 [millions-bitcoin-sim-swapping](#) “SIM swapping consists of tricking a provider like
2 AT&T or T-Mobile into transferring the target’s phone number to a SIM card
3 controlled by the criminal. Once they get the phone number, fraudsters can
4 leverage it to reset the victims’ passwords and break into their online accounts
5 (cryptocurrency accounts are common targets.) In some cases, this works even if
6 the accounts are protected by two-factor authentication. This kind of attack, also
7 known as ‘port out scam,’ is relatively easy to pull off and has become widespread,
8 as a recent Motherboard investigation showed.”

9 54. The leading security reporter Brian Krebs wrote on August 18,
10 2018 ([https://krebsonsecurity.com/2018/08/florida-man-arrested-in-sim-swap-](https://krebsonsecurity.com/2018/08/florida-man-arrested-in-sim-swap-conspiracy/)
11 [conspiracy/](#)) that “SIM swaps are frequently abused by scam artists who trick
12 mobile providers into tying a target’s service to a new SIM card and mobile phone
13 that the attackers control. Unauthorized SIM swaps often are perpetrated by
14 fraudsters who have already stolen or phished a target’s password, as many banks
15 and online services rely on text messages to send users a one-time code that needs
16 to be entered in addition to a password for online authentication.” As Mr. Krebs
17 also wrote: “[i]n some cases, fraudulent SIM swaps succeed thanks to lax
18 authentication procedures at mobile phone stores. *In other instances, mobile store*
19 *employees work directly with cyber criminals to help conduct unauthorized SIM*
20 *swaps. . . .*” (Emphasis added.)

21 55. Mr. Terpin alleges on information and belief that AT&T knew
22 well before the attacks on Mr. Terpin that it was subject to widespread SIM swap
23 fraud. Mr. Terpin alleges further that AT&T knew that cryptocurrency investors
24 like Plaintiff were specifically targeted by SIM swapping and that AT&T was the
25 weak link in such fraud. This is confirmed in numerous articles on SIM swap
26 fraud, including that of Brian Krebs and a July 31, 2018 article in bitcoinist.com
27 entitled “Sim-Swapping Bitcoin Thief Charged in California Court,” available at
28 <https://bitcoinist.com/sim-swapping-bitcoin-thief-charged-california-court/>. The

1 bitcoinist.com article states that “the liability for [SIM swapping] attacks [lies]
2 squarely at the feet of the service providers [which the article calls the ‘weakest
3 link’] as security procedures for confirming identity should not be bypass-able
4 using a few pieces of personal information easily obtained online.”

5 56. Mr. Terpin also alleges on information and belief that AT&T
6 knew or should have known that its employees frequently cooperated with hackers
7 and thieves to bypass its security procedures. This is confirmed not only by Brian
8 Krebs, who wrote that “mobile store employees work directly with cyber
9 criminals,” but in an August 3, 2018 article in *Motherboard* entitled “How
10 Criminals Recruit Telecom Employees to Help them Hijack SIM Cards,” available
11 at [https://motherboard.vice.com/en_us/article/3ky5a5/criminals-recruit-telecom-](https://motherboard.vice.com/en_us/article/3ky5a5/criminals-recruit-telecom-employees-sim-swapping-port-out-scam)
12 [employees-sim-swapping-port-out-scam](https://motherboard.vice.com/en_us/article/3ky5a5/criminals-recruit-telecom-employees-sim-swapping-port-out-scam), which describes how scammers routinely
13 recruit and pay employees of AT&T and other Telecoms called “plugs” to perform
14 illegal SIM swaps.

15 57. Mr. Terpin further alleges on information and belief that despite
16 its knowledge that its employees actively cooperate with hackers to rob its own
17 customers, AT&T has done nothing to prevent such scams. As an AT&T employee
18 confirmed in the August 3, 2018 *Motherboard* article, “if a criminal finds a corrupt
19 insider, ‘there aren’t enough safeguards [in place] to stop that employee,’ . . .” The
20 AT&T employee further told the author of the article that “*the system is designed so*
21 *that some employees have the ability to override security features such as the phone*
22 *passcode that AT&T (and other companies) now require when porting numbers.*
23 ‘From there the passcode can be changed,’ the employee said in an online chat,
24 referring to a customer information portal that they showed *Motherboard*. ‘With a
25 fresh passcode the number can be ported out with no hang ups.’” (Emphasis
26 added.)

27 58. Mr. Terpin alleges on information and belief that countless
28 AT&T customers have been the victims of SIM swapping and that those customers

1 have lost hundreds of millions of dollars or more because of the fraud. This is
2 confirmed by the July 30, 2018 *Motherboard* article, which describes the arrest of
3 Joel Ortiz, one of a group of criminals from Boston, who “used the increasingly
4 popular technique known as SIM swapping or SIM hijacking to steal bitcoin, other
5 cryptocurrencies and social media accounts.” In a fraud that mirrors the one
6 suffered by Mr. Terpin some months earlier, Ortiz “*specifically targeted people*
7 *involved in the world of cryptocurrency and blockchain*,” including in an incident
8 where he *stole more than \$1.5 million from a cryptocurrency entrepreneur who was*
9 *an AT&T customer.*” (Emphasis added)

10 59. This is further confirmed in the August 18, 2018 article by Brian
11 Krebs, which describes the arrest of Ricky Joseph Handschumacher in Florida, who
12 was charged with grand theft and money laundering for draining cryptocurrency
13 accounts through SIM fraud. According to Krebs, Handschumacher’s group came
14 to light “when a Michigan woman called police after she overheard her son talking
15 on the phone and pretending to be an AT&T employee. Officers responding to the
16 report searched the residence and found multiple cell phones and SIM cards, as well
17 as files on the kid’s computer that included ‘an extensive list of names and phone
18 numbers of people from around the world.’”

19 60. Krebs’ report further revealed that “[t]he Pasco County [Florida]
20 Sheriff’s office says their surveillance of the Discord [voice chat] server revealed
21 that the group *routinely paid employees at cellular phone companies to assist in*
22 *their attacks, and that they even discussed a plan to hack accounts belonging to the*
23 *CEO of cryptocurrency exchange Gemini Trust Company.*” (Emphasis added.)

24 61. Mr. Terpin alleges on information and belief that AT&T is fully
25 aware of these and numerous other SIM swapping incidents involving its
26 customers, including incidents where its own employees were complicit with
27 hackers. For example, the *Motherboard* article confirms that AT&T had provided
28 investigators with the victim’s call records “for the days when the hacker was

1 allegedly in control of the investor's numbers." Indeed, those records were used by
2 law enforcement in issuing a warrant for e-mails from the phone which produced
3 incriminating evidence against Ortiz.

4 62. Mr. Terpin further alleges on information and believe that
5 federal enforcement agencies have compiled proof that insiders at AT&T
6 cooperated in SIM swap fraud that was directed at members of the cryptocurrency
7 community. Mr. Terpin further alleges that such insiders actively cooperated with
8 hackers to provide them customer list information.

9 63. The prevalence of SIM swap fraud and AT&T's knowledge of
10 such fraud, including the active participation of its own employees in the fraud,
11 demonstrate that the January 7, 2018 SIM swap fraud on Mr. Terpin that led to the
12 theft of nearly \$24 million in cryptocurrency was neither an isolated nor an
13 unforeseeable event.

14 **THE JUNE 11, 2017 HACK**

15 64. On or about June 11, 2017, Mr. Terpin discovered that his
16 AT&T cell phone number had been hacked when his phone suddenly became
17 inoperable. As Mr. Terpin learned from AT&T a few days later, his AT&T
18 password had been changed remotely after 11 attempts in AT&T stores had failed.
19 By obtaining control over Mr. Terpin's phone, the hackers diverted Mr. Terpin's
20 personal information, including telephone calls and text messages, to get access to
21 accounts that use telephone numbers as a means of verification or authentication.

22 65. After the hackers took charge of Mr. Terpin's telephone number,
23 the hackers accessed Mr. Terpin's telephone to divert texts and telephone calls to
24 gain access to Mr. Terpin's cryptocurrency accounts. The hackers also used the
25 phone to hijack Mr. Terpin's Skype account to impersonate him. By that means,
26 the hackers convinced a client of Mr. Terpin to send them cryptocurrency and
27 diverted a payment due to Mr. Terpin to themselves. AT&T finally cut off access
28

1 by the hackers to Mr. Terpin's telephone number on June 11, 2017, but only after
2 the hackers had stolen substantial funds from Mr. Terpin. Moreover, because of the
3 hack, Mr. Terpin expended a substantial amount of time investigating the hack and
4 attempting to repair his computer accounts.

5 66. On or about June 13, 2017, Mr. Terpin met with AT&T
6 representatives in Puerto Rico to discuss the June 11, 2017 hack. Mr. Terpin
7 explained to AT&T that he had been hacked and that the hackers had stolen a
8 substantial amount of money from him. Mr. Terpin expressed concern about
9 AT&T's ineffective security protections and asked how he could protect the
10 security of his phone number and account against future unauthorized access,
11 including hackers attempting to perpetrate SIM swap fraud.

12 67. In response to Mr. Terpin's request for greater security for his
13 account, AT&T promised that it would place his account on a "higher security
14 level" with "special protection." AT&T told Mr. Terpin that this "higher security
15 level" would require anyone accessing or changing Mr. Terpin's account to provide
16 a six-digit passcode to AT&T to access or change the account. Anyone requesting
17 AT&T to transfer Mr. Terpin's telephone number to another phone must provide
18 the code. AT&T promised Mr. Terpin at this meeting that the higher security that
19 it was placing on his account, which it also called "high risk" or "celebrity"
20 protection, would insure that Mr. Terpin's account was much less likely to be
21 subject to SIM swap fraud. AT&T further told Mr. Terpin that the implementation
22 of the increased security measures would prevent Mr. Terpin's number from being
23 moved to another phone without Mr. Terpin's explicit permission, because no one
24 other than Mr. Terpin and his wife would know the secret code.

25 68. At alleged above, AT&T was well aware at the time of the June
26 11, 2017 incident that its users were subject to SIM swap fraud. It was also well
27 aware that its employees cooperated in such fraud and that the employees could
28 bypass its security procedures. Mr. Terpin alleges on information and belief that

1 AT&T had been previously contacted numerous times by law enforcement
2 authorities about such frauds involving its own employees who actively cooperated
3 with hackers. Nonetheless, AT&T recommended that customers who were
4 concerned about fraudulent actions on their account add purported “extra security”
5 by adding a “wireless security password” to protect their account. AT&T touted
6 the benefits of such “extra” security on its website because it would require a
7 password for “*managing your account in any retail store.*” See
8 <https://www.att.com/esupport/article.html#!/wireless/KM1051397> (emphasis
9 added).

10 69. Mr. Terpin relied upon AT&T’s promises that his account
11 would be much more secure against hacking, including SIM swap fraud, after it
12 implemented the increased security measures. Because of the implementation of
13 such measures, Mr. Terpin retained his account with AT&T. But for these express
14 promises and assurances, Mr. Terpin would have canceled his AT&T account and
15 contracted with a different cellular telephone provider and he would not have lost
16 nearly \$24 million from hackers.

17 70. Mr. Terpin further alleges on information and belief that AT&T
18 knew at the time that it recommended that he adopt additional security on his
19 account that the additional security measures were not adequate and could be
20 overridden by its employees. In reality, the vaunted extra protection was, like the
21 Maginot Line, a useless defense that was easily evaded by AT&T’s own
22 employees, who it knew or should have known actively cooperated with hackers in
23 SIM swap fraud. Despite AT&T’s knowledge of the futility of these actions,
24 AT&T falsely informed Mr. Terpin, to his detriment, that he should implement
25 such additional security measures.

26 **THE JANUARY 7, 2018 SIM SWAP FRAUD**

27 71. AT&T’s promises proved to be false and the increased security
28 illusory. On Sunday January 7, 2018, an employee in an AT&T store cooperated

1 with an imposter committing SIM swap fraud. Unbeknownst to Mr. Terpin, AT&T
2 had grossly misrepresented its ability to secure Mr. Terpin's Personal Information
3 after the June 11, 2017 incident. Not only had AT&T failed to disclose that it did
4 not properly supervise, train or monitor its employees to ensure that they
5 scrupulously followed AT&T's security procedures, but it also failed to disclose
6 that it knew that its employees could readily bypass the higher security protection
7 placed on Mr. Terpin's account after the June 11, 2017 hack.

8 72. On January 7, 2018, Mr. Terpin's phone with his AT&T
9 wireless number went dead. Mr. Terpin was again a victim of SIM swap fraud. As
10 AT&T later admitted, an employee in an AT&T store in Norwich, Connecticut
11 ported over Mr. Terpin's wireless number to an imposter in violation of AT&T's
12 commitments and promises, including the higher security that it had supposedly
13 placed on Mr. Terpin's account after the June 11, 2017 hack that had supposedly
14 been implemented to prevent precisely such fraud. Through the January 7, 2018
15 hack, thieves gained control over Mr. Terpin's accounts and stole nearly \$24
16 million worth of cryptocurrency from him on January 7 and 8, 2018.

17 73. When Mr. Terpin's telephone went dead on January 7, 2018, he
18 instantly attempted to contact AT&T to have the telephone number immediately
19 canceled so that the hackers would not gain access to his Personal Information and
20 accounts. Ignoring Mr. Terpin's urgent request, AT&T failed promptly to cancel
21 Mr. Terpin's account, which gave the hackers sufficient time to obtain information
22 about Mr. Terpin's cryptocurrency holdings and to spirit off funds to their own
23 accounts. Adding insult to injury, AT&T placed Mr. Terpin's wife on endless hold
24 (over an hour!) when she asked to be connected to AT&T's fraud department while
25 Mr. Terpin was furiously attempting to see what damage was being done to his
26 accounts. Mr. Terpin's wife never reached AT&T's fraud department because it
27 apparently does not work (or is unavailable) on Sundays. But the hackers work on
28 Sunday!

1 74. The employees at the AT&T store who unlawfully handed over
2 Mr. Terpin's telephone number to thieves were either blind or complicit. It was
3 impossible to look at Mr. Terpin's account information on the AT&T computer
4 screen and not see the multiple warnings about the need for heightened vigilance,
5 particularly the requirement of a six-digit password. Nonetheless, as AT&T had
6 reason to know before the January 7, 2018 incident (but had never informed Mr.
7 Terpin or other customers), its employees could readily bypass its much-touted
8 security procedures.

9 75. In cooperating willingly with hackers committing SIM swap
10 fraud to plunder Mr. Terpin's accounts, AT&T violated its own policies as well as
11 the requirements of Section 222 of the FCA and the FCC Consent Decree. On
12 information and belief, AT&T knew that its employees were frequently complicit
13 with SIM swap frauds and could readily bypass its security procedures. Mr. Terpin
14 further alleges that AT&T did not even attempt to require the hacker to provide the
15 six-digit code that AT&T required for access to Mr. Terpin's "high profile" account
16 or to require a supervisor to approve the manual override. Indeed, AT&T admitted
17 to Mr. Terpin on February 4, 2018 that a sales associate in AT&T's Norwich,
18 Connecticut location had violated AT&T's procedures by not only failing to ask for
19 the six-digit code, but also by bypassing its requirement that the hacker have a
20 scannable ID to obtain a replacement SIM card for Mr. Terpin's wireless number.
21 On information and belief, Mr. Terpin alleges that the employee in the AT&T store
22 who handed over the SIM card to the imposter had a criminal record and was
23 cooperating with the hacker and that AT&T had failed properly to supervise the
24 employee, despite its knowledge that its employees cooperated in precisely this
25 type of fraud.

26 76. Because of AT&T's cooperation and failure to follow its own
27 policies, the hackers were able to intercept Mr. Terpin's personal information,
28

1 including telephone calls and text messages, and gain access to his cryptocurrency
2 accounts.

3 77. Because of AT&T's willing cooperation with the hacker, gross
4 negligence, violation of its statutory duties, and failure to adhere to its
5 commitments in its Privacy Policy and COBC, as well as its obligations under the
6 FCC Consent Degree and its commitments to Mr. Terpin after the June 11, 2017
7 hack, Mr. Terpin lost nearly \$24 million worth of cryptocurrency.

8 78. To Mr. Terpin's knowledge, AT&T never informed either the
9 FCC, the FBI or any other law enforcement or regulatory authority about the
10 January 7, 2018 SIM swap. Nor did AT&T ever provide Mr. Terpin with a written
11 explanation of how the SIM swap fraud occurred or a claim form, let alone an
12 apology for facilitating the hack. In contrast, Mr. Terpin himself reported the
13 January 7, 2018 SIM swap to the FBI and the Secret Service Cyber Crimes Unit
14 and has actively sought an investigation of the hack and recovery of the stolen
15 funds. To date, Mr. Terpin has not been able to recover any of the funds that were
16 stolen.

17 79. On information, Mr. Terpin alleges that AT&T did not
18 discipline or terminate the employee who turned over a SIM card for his telephone
19 number to imposters and who facilitated the theft of nearly \$24 million worth of
20 Mr. Terpin's cryptocurrency.

21 **FIRST CLAIM FOR RELIEF**

22 **(Declaratory Relief:**

23 **Unenforceability of AT&T Consumer Agreement as Unconscionable and** 24 **Contrary to Public Policy)**

25 80. Mr. Terpin brings this claim for declaratory relief under 28
26 U.S.C. § 2201 to have the Court declare that AT&T's wireless customer agreement
27 (the "Agreement") is unconscionable, void against public policy under Cal. Civ.
28 Code §§ 1670.5 and 1668, and unenforceable in its entirety.

1 81. Mr. Terpin initially entered into a wireless contract with AT&T
2 in or about 2011 when he transferred the account from his wife. Mr. Terpin has
3 asked AT&T for a copy of his agreement, but AT&T refused to provide it to him.
4 Mr. Terpin thus has no copy of any agreement with AT&T for wireless services.

5 82. The agreement was presented to Mr. Terpin, like all other
6 wireless users, on a take-it-or-leave-it basis. Mr. Terpin had no ability to negotiate
7 any term of the agreement. In contrast, AT&T has virtually unlimited power over
8 its customers, including Mr. Terpin, as seen below by the fact that it purports to
9 hold Mr. Terpin and all other wireless users to the terms of an agreement that they
10 may well have never seen or read.

11 83. The version of the Agreement posted in early 2018 purports to
12 govern AT&T's provision of wireless service to all customers, including Mr.
13 Terpin who first contracted with AT&T over two decades ago. A true and correct
14 copy of the Agreement posted on AT&T's website in early 2018 at
15 <https://www.att.com/legal/terms.wirelessCustomerAgreement-list.html> is attached
16 hereto as Exhibit D. As alleged below, the Agreement contains numerous
17 unconscionable terms that renders it unenforceable in its entirety because its
18 "central purpose . . . is tainted with illegality." *Ingle v. Circuit City Stores, Inc.*,
19 328 F.3d 1165, 1180 (9th Cir. 2003) (holding invalid an agreement that obstructs the
20 ability of customers to bring any claims against defendant).

21 84. The Agreement states that the Agreement and other agreements
22 that are "not otherwise described below that are posted on applicable AT&T
23 websites or devices, and any documents expressly referred to herein or therein,
24 make up the complete agreement between you and AT&T and supersede any and
25 all prior agreements and understandings relating to the subject matter of this
26 Agreement." Through such vague language, AT&T apparently contends that not
27 only the Agreement, but other unspecified and unknown agreements, bind all
28 wireless customers, whether or not such customers have seen the Agreement or are

1 aware of its terms. In other words, every time AT&T mints a new (and more
2 onerous) version of its agreements, its unsuspecting customers are purportedly
3 bound by the new terms. This practice highlights the fact that not only are these
4 contracts not negotiable, they are invisible. What you don't see, you still get.

5 85. The Agreement is a classic contract of adhesion imposed by
6 AT&T upon a party with no bargaining power. In contrast, AT&T has unchecked
7 power to insist upon its own terms even if the consumer is unaware of the terms of
8 the Agreement itself. There is no ability to negotiate any term of the Agreement. It
9 is literally "take it or leave it."

10 86. The Agreement is void as against public policy under Cal. Civ.
11 Code § 1668 as a contract of adhesion purporting to bind customers who have never
12 heard or seen the agreement and most likely are entirely unaware of its provisions.
13 The Agreement is void and unenforceable in its entirety because it also contains
14 exculpatory provisions, damage waivers, and an indemnification provision that
15 purport to prevent consumers from bringing *any* claims against AT&T or obtaining
16 redress for their claims -- even for billing errors.

17 87. The exculpatory provision in Paragraph 4.1 of the Agreement
18 ("Exculpatory Provision") contains numerous provisions that are contrary to public
19 policy under Cal. Civ. Code § 1668 because they attempt to exempt AT&T from
20 responsibility for its own gross negligence, fraud, and violations of law. In
21 pertinent part, the Exculpatory Provision states that:

22 ***WE DO NOT GUARANTEE YOU UNINTERRUPTED SERVICE***
23 ***OR COVERAGE. . . . AT&T MAKES NO WARRANTY,***
24 ***EXPRESS OR IMPLIED, OF MERCHANTABILITY OR FITNESS***
25 ***FOR A PARTICULAR PURPOSE, SUITABILITY, ACCURACY,***
26 ***SECURITY OR PERFORMANCE REGARDING ANY SERVICES,***
27 ***SOFTWARE OR GOODS, AND IN NO EVENT SHALL AT&T BE***
28

1 ***LIABLE, WHETHER OR NOT DUE TO ITS OWN NEGLIGENCE,***

2 for any:

3 a. act or omission of a third party;

4 b. mistakes, omissions, interruptions, errors, failures to transmit,
5 delays, or defects in the Services or Software provided by or through
6 us;

7 c. ***damages or injury caused by the use of Services, Software, or***
8 ***Device***, including use in a vehicle . . .

9 (Capitalization in original; emphasis added in bold and italics.)

10 88. The Exculpatory Provision renders the entire Agreement
11 unenforceable on public policy grounds under Cal. Civil Code §§ 1668 and 1670.5
12 because it purports to exempt AT&T from its gross negligence, statutory violations
13 and willful behavior, including the egregious conduct alleged herein. The
14 Exculpatory Provision is further against public policy because it purports to exempt
15 AT&T from violation of statutory obligations, including the obligation to maintain
16 the confidentiality and security of its customers' private and personal information
17 under Section 222 of the FCA, the FCC Consent Degree, and numerous provisions
18 of California State law, including California unfair competition law, the Consumer
19 Legal Remedies Act, and the California Customer Records Act. Thus, even where,
20 as here, AT&T willfully violates its statutory duties under the FCA and the Consent
21 Decree, not to mention its promises in its Privacy Policy and the COBC, a customer
22 is prevented by the Exculpatory Provision from bringing a claim for negligent or
23 willful disclosure of the customer's Personal Information, including CPNI, because
24 such claim seeks redress for "damages or injury caused by the use of Services,
25 Software, or Device . . ." and is waived by the Exculpatory Provision.

26 89. AT&T also seeks in the contract to have customers waive any
27 damages, except for providing a "credit equal to a pro-rata adjustment of the
28

1 monthly Services fee for the time period your Services was unavailable, not to
2 exceed the monthly Service fee” when a customer’s services are interrupted.

3 90. Section 4.1 of the Agreement (“Damages Restriction”) is also
4 void under Cal. Civ. Code §§ 1668 and 1670.5 because it purports to exempt
5 AT&T for all other damages:

6 Unless prohibited by law, AT&T isn’t liable for any indirect, special,
7 punitive, incidental or consequential losses or damages you or any
8 third party may suffer by use of, or inability to use, Services, Software
9 or Devices provided by or through AT&T, including loss of business
10 or goodwill, revenue or profits, or claims of personal injuries.

11 91. The Exculpatory Provision is invalid under Civil Code § 1670.5
12 because it allocates all the risks to the consumer with AT&T disclaiming any
13 damages for its own conduct—even fraud, gross negligence, and statutory
14 violations, including those governed by the FCA. Thus, even if AT&T deliberately
15 handed over a customer’s CPNI to hackers in violation of Section 222 of the FCA,
16 a customer would not be entitled to the full range of damages afforded by that
17 statute under the Damages Restriction.

18 92. The Damages Restriction included in a contract of adhesion as
19 to which AT&T’s users, including Mr. Terpin, have no bargaining authority, is void
20 because it is plainly unconscionable and against public policy. The Damages
21 Restriction is contained in a lengthy form contract drafted by a domineering
22 telecommunication provider with vast assets in a far superior bargaining position to
23 the wireless user. Indeed, it is no exaggeration to say that the consumer has no
24 bargaining power as regards AT&T, particularly as to the Damages Restriction and
25 other draconian provisions in the Agreement. Because the Damages Restriction is
26 found in a document posted on a website that, by fiat, is automatically made
27 applicable to customers, customers may not even be aware that they have virtually
28 no redress against AT&T, unless they diligently monitor changes in the website.

1 Moreover, the Damages Restriction is contained in a complex and lengthy contract
2 that provides essential wireless services—without which most customers have no
3 means of communication (including for emergency services), let alone essential
4 computing, geolocation, texting, research or other services.

5 93. The Damages Restriction is also substantively unconscionable
6 because it allocates risks in an objectively unreasonable manner. *See Armendariz v.*
7 *Foundation Health Psychcare Services, Inc.*, 24 Cal. 4th 83, 113-114 (2000). The
8 allocation of risks under the Agreement is objectively unreasonable because
9 AT&T—a telecommunications behemoth with billions of dollars of assets and tens
10 of millions of customers—takes upon itself virtually no liability (other than
11 minimal recompense for interrupted services) and purports to exempt itself from
12 virtually all damages, including those arising out of its own deliberate, grossly
13 negligent, or fraudulent acts.

14 94. The Agreement is further unenforceable because customers are
15 purportedly required to indemnify AT&T for all claims arising out of the services
16 provided by AT&T, including claims that arise due to AT&T’s negligence, gross
17 negligence, deliberate conduct, or statutory violations. The indemnity provision in
18 Paragraph 4.1 of the Agreement (“Indemnity”) states:

19 To the full extent allowed by law, you hereby release, indemnify, and
20 hold AT&T and its officers, directors, employees and agents harmless
21 from and against *any and all claims of any person or entity for*
22 *damages of any nature arising in any way from or relating to, directly*
23 *or indirectly, service provided by AT&T or any person’s use thereof*
24 (including, but not limited to vehicular damage and personal injury),
25 *INCLUDING CLAIMS ARISING IN WHOLE OR IN PART FROM*
26 *THE ALLEGED NEGLIGENCE OF AT&T*, or any violation by you of
27 this Agreement.

28 (Capitalization in original; emphasis added.)

1 95. Read literally, the Indemnity requires a consumer, such as Mr.
2 Terpin, to hold AT&T harmless for AT&T's own negligence, deliberate behavior,
3 gross negligence, statutory violations (including disclosure of CPNI under the
4 FCA), or fraud if the conduct is related "directly or indirectly" to any "service
5 provided by AT&T." On its face, the indemnity provision in a contract of adhesion
6 renders the entire Agreement unconscionable and unenforceable because it defeats
7 the entire purpose of the contract by making it impossible for consumers to bring
8 claims against AT&T for the entire range of statutory rights to which a consumer,
9 such as Mr. Terpin, is entitled. Indeed, the Indemnity would totally obviate
10 AT&T's commitment to privacy in its Privacy Policy as well as its legal obligations
11 under the FCA, the CPNI Rules, and the Consent Decree.

12 96. Because the entire Agreement is unenforceable because the
13 central purpose of the Agreement is "tainted with illegality . . . [so that] the contract
14 as a whole cannot be enforced," the arbitration provision in Paragraph 2.2 of the
15 Agreement ("Arbitration Provision") is also enforceable. *See, Armendariz*, 24 Cal.
16 4th at 89-90.

17 97. The Arbitration Provision would require Mr. Terpin to arbitrate
18 his claims "without affording the full range of statutory remedies, including
19 punitive damages and attorney fees" that are available to him under the claims
20 alleged herein. *Armendariz*, 24 Cal. 4th at 103 (damages limitation unlawful if
21 applied to statutory claims). For example, Mr. Terpin, if required to arbitrate this
22 claim, would be forced by the Damages Limitation to forego his statutory
23 entitlement to punitive damages under his Third Claim for Relief under California
24 Penal Code § 502 *et seq.* and to his entitlement to punitive damages for AT&T's
25 fraud and negligence. Moreover, the Arbitration Provision would require Mr.
26 Terpin to forego the full range of damages to which he is entitled under his Second
27 Claim for Relief under the Federal Communications Act § 222. These defects
28

1 render not only the Arbitration Provision, but also the entire Agreement,
2 unenforceable.

3 98. Because the defenses raised by Mr. Terpin as to the
4 unconscionability of the Agreement are “enforced evenhandedly” and do not
5 “interfere[] with the fundamental attributes of arbitration,” they do not run afoul of
6 *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333 (2010). The Court’s decision in
7 *Concepcion* did not abrogate the savings clause of the FAA that provides that
8 arbitration agreements may be declared unenforceable “upon such grounds as exist
9 at law or in equity for the revocation of any contract,” including “generally
10 applicable contract defenses, such as fraud, duress, or unconscionability.”
11 *Concepcion* at 339, quoting 9 U.S.C. § 2 and *Doctors Associates, Inc. v. Casarotto*,
12 517 U.S. 681, 687 (1996). For the reasons alleged in this claim, such defenses
13 apply squarely to the Agreement.

14 99. There is an actionable and justiciable controversy between Mr.
15 Terpin and AT&T in that Mr. Terpin contends that the Agreement, including the
16 Exculpatory Provision, Damages Restriction, Indemnity and Arbitration Provision,
17 is unenforceable in its entirety because it is unconscionable and void against public
18 policy since it prevents consumers, such as Mr. Terpin, from obtaining redress
19 against AT&T even for deliberate acts in violation of its legal duties. AT&T
20 undoubtedly disagrees.

21 100. A judicial declaration of the enforceability of the Agreement,
22 including the Exculpatory Provision, Damages Restriction, Indemnity and
23 Arbitration Provision and all other provisions of the Agreement, is necessary and
24 appropriate.

25 101. Mr. Terpin seeks a judgment declaring that the Agreement in its
26 entirety is unenforceable as unconscionable and against public or, in the alternative
27 that (a) the Exculpatory Provision is unenforceable as against Mr. Terpin; (b) the
28 Damages Restriction is unenforceable against Mr. Terpin; (c) the Indemnity is

unenforceable as against Mr. Terpin; and (d) the Arbitration Provision is unenforceable as against Mr. Terpin

SECOND CLAIM FOR RELIEF

(Unauthorized Disclosure of Customer Confidential Proprietary Information and Proprietary Network Information (Federal Communications Act, 47 U.S.C. §§ 206, 222))

102. Plaintiff realleges the allegations in Paragraphs 1-101 as if fully set forth herein.

103. AT&T is a “common carrier” engaging in interstate commerce by wire regulated by the Federal Communications Act (“FCA”) and subject to the requirements, *inter alia*, of sections 206 and 222 of the FCA.

104. Under section 206 of the FCA, 47 U.S.C. § 206, “[i]n case any common carriers shall do, or cause or permit it to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done, such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter, together with a reasonable counsel or attorney’s fee, to be fixed by the court in every case of recovery, which attorney’s fee shall be taxed and collected as part of the costs in the case.”

105. Section 222(a) of the FCA, 47 U.S.C. § 222(a), requires every telecommunications carrier to protect, among other things, the confidentiality of proprietary information of, and relating to, customers (“CPI”).

106. Section 222(c)(1) of the FCA, 47 U.S.C. § 222(c)(1) further requires that, “[e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to customer proprietary network information

1 ['CPNI'] in its provision of (A) telecommunications services from which such
2 information is derived, or (B) services necessary to or used in the provision of such
3 telecommunication services. . . .”

4 107. The information disclosed to hackers by AT&T in the January 7,
5 2018 SIM swap fraud transferring Mr. Terpin’s telephone number, was CPI and
6 CPNI under Section 222 of the FCA.

7 108. AT&T failed to protect the confidentiality of Mr. Terpin’s CPI
8 and CPNI, including his wireless telephone number, account information, and his
9 private communications, by divulging that information to hackers in the January 7,
10 2018 SIM swap fraud. Through its negligence, gross negligence and deliberate
11 acts, including inexplicable failures to follow its own security procedures, supervise
12 its employees, the CPNI Regulations, the terms of the Consent Decree, the
13 warnings of the Pretexting Order, its Privacy Policy and the COBC, and by
14 allowing its employees to bypass such procedures, AT&T permitted hackers to
15 access Mr. Terpin’s telephone number, telephone calls, text messages and account
16 information to steal nearly \$24,000,000 worth of his cryptocurrency.

17 109. As a direct consequence of AT&T’s violations of the FCA, Mr.
18 Terpin has been damaged by loss of nearly \$24,000,000 worth in cryptocurrency
19 which AT&T allowed to fall into the hands of thieves, and for other damages in an
20 amount to be proven at trial.

21 110. Mr. Terpin is also entitled to his attorney’s fees under the FCA
22 in bringing this action against AT&T for its gross negligence and fraudulent
23 misrepresentation as to the security that it provides for customer accounts as
24 required by the FCA, the CPNI Regulation, and the Consent Decree.

THIRD CLAIM FOR RELIEF

(Assisting Unlawful Access to Computer

California Penal Code § 502 *et seq.*)

111. Mr. Terpin realleges the allegations in Paragraphs 1-110 as if fully set forth herein.

112. AT&T violated California Penal Code § 502 *et seq.* by knowingly and without permission allowing unauthorized third parties to access Mr. Terpin's computers, computer systems and computer networks, including his mobile phone.

113. As herein alleged, AT&T on or about January 7, 2018 transferred Mr. Terpin's telephone number to unauthorized individuals who used it to access his computer systems and accounts.

114. When AT&T handed over Mr. Terpin's wireless number and account to unauthorized individuals, AT&T was on notice that Mr. Terpin's Personal Information was vulnerable to attack because it was aware of the prevalence of SIM swap fraud, pretexting scams, and its employees' misconduct, including as detailed in the Consent Decree. AT&T was also aware that Mr. Terpin was vulnerable because he had contacted AT&T after the June 11, 2017 incident and AT&T had placed additional "high security" safeguards on Mr. Terpin's account to guard against potential future attacks. In addition to other mandated procedures, these safeguards included requiring anyone who wished to access Mr. Terpin's account in an AT&T store to provide a six-digit passcode.

115. Although AT&T was aware of the necessity for safeguards for its customers' Personal Information under the FCA, CPNI Rules, and the Consent Decree, and had made specific commitments to Mr. Terpin after the June 11, 2017 incident that it was placing additional security on Mr. Terpin's accounts, AT&T on January 7, 2018 did not require the unauthorized individual to provide it with the required six-digit passcode or legally proper identification and allowed its

1 employee to bypass the protections on Mr. Terpin's account. Instead, AT&T
2 cooperated with the hackers by porting over Mr. Terpin's wireless number to
3 telephones controlled by hackers that then allowed them to access Mr. Terpin's
4 Personal Information, including CPNI.

5 116. AT&T's blatant disregard of its high security procedures and
6 willing cooperation with the hackers on January 7, 2018 constitutes knowing
7 cooperation with unauthorized individuals accessing Mr. Terpin's computers,
8 computer systems, and computer networks. AT&T knew from the June 11, 2017
9 incident that Mr. Terpin was a high-profile target and that hackers had accessed Mr.
10 Terpin's computers, computer systems, and computer networks. Mr. Terpin further
11 alleges on information and belief that it knew that individuals in the crypto currency
12 community were particularly subject to SIM swap fraud and that its employees
13 actively cooperated with such hackers to victimize its own customers.

14 117. AT&T further knew that the hackers to whom it ported Mr.
15 Terpin's telephone number on January 7, 2018 were not authorized to access Mr.
16 Terpin's Personal Information because the hackers did not have identification
17 conforming to AT&T's or the FCC's requirements under the CPNI Rule. Indeed,
18 on January 7, 2018 AT&T handed over Mr. Terpin's telephone number and
19 Personal Information even though the hackers further lacked the required "high
20 security" six-digit code required to access or modify Mr. Terpin's wireless account.

21 118. Because of AT&T's knowing cooperation with the hackers in
22 the January 7, 2018 SIM swap fraud, AT&T provided the hackers with means to
23 access Mr. Terpin's computers, computer systems, and computer networks and to
24 steal nearly \$24 million worth of cryptocurrency from Mr. Terpin.

25 119. What is truly mystifying here is how the hacker for the January
26 7, 2018 crime could get Mr. Terpin's telephone number on the first try. Back on
27 July 11, 2017, the criminals were unable to get the number even though they visited
28 11 stores. Most likely, as AT&T knew, the January 7, 2018 hacker was an inside

1 job facilitated by a “plug” employee at the AT&T facility! Either way, AT&T is
2 left holding the bag.

3 120. Because of the conduct alleged herein by AT&T, Mr. Terpin is
4 entitled to compensatory damages and injunctive relief under Penal Code §
5 502(e)(1). Mr. Terpin is also entitled to reasonable attorney fees pursuant to Penal
6 Code § 502(e)(2).

7 121. Because AT&T’s conduct as alleged herein is willful and was
8 conducted with oppression, fraud or malice as defined in Civil Code § 3294(c), Mr.
9 Terpin is entitled to punitive or exemplary damages in an amount to be proven at
10 trial.

11 **FOURTH CLAIM FOR RELIEF**
12 **(Violation of California Unfair Competition Law**
13 **Unlawful Business Practice**

14 **Cal. Bus. & Prof. Code § 17200 *et seq.*)**

15 122. Plaintiff realleges the allegations in Paragraphs 1-121 as if fully
16 stated herein.

17 123. Because of the conduct alleged herein, AT&T engaged in
18 unlawful practices within the meaning of the California Unfair Competition Law
19 (“UCL”), Cal. Bus. & Prof. Code § 17200 *et seq.* The conduct alleged herein is a
20 “business practice” within the meaning of the UCL.

21 124. AT&T stored and processed Mr. Terpin’s Personal Information,
22 including CPI and CPNI, in its electronic systems and databases. Mr. Terpin’s
23 CPNI and other Personal Information could readily be accessed when Mr. Terpin’s
24 telephone number was ported out to a new telephone controlled by a hacker. All
25 such information is “Personal Information” under AT&T’s Privacy Policy.

26 125. AT&T falsely represented to Mr. Terpin and other customers in
27 its Privacy Policy and COBC: (a) that its system was secure and that it would
28 respect the privacy of its customers’ information; (b) that it had “established

1 electronic and administrative safeguards designed to make the information we
2 collect secure,” as well as requiring employees to adhere to the COBC and other
3 codes of conduct, including “the legal requirements and company policies
4 surrounding the privacy of communications and the security and privacy of your
5 records”; and (c) that it had “implemented technology and security features and
6 strict policy guidelines to safeguard the privacy of your Personal information,”
7 including “[l]imiting access to Personal Information to only those with jobs
8 requiring such access” and “[r]equiring caller/online authentication before
9 providing Account Information so that only you or someone who knows your
10 Account Information will be able to access or change this information.” These
11 security measures and safeguards included those mandated by the CPNI Rules and
12 Consent Decree.

13 126. AT&T knew or should have known that it did not employ
14 reasonable, industry standard and appropriate security measures that complied with
15 “legal requirements,” in the FCA, CPNI Rules, Consent Decree and other laws and
16 regulations. AT&T also knew from the FCC investigation leading to the Consent
17 Decree that its employee monitoring and training was inadequate.

18 127. AT&T misrepresented to Mr. Terpin after the June 11, 2017
19 incident that it had added “special protection” to protect Mr. Terpin’s “celebrity” or
20 “high profile” account. These increased security measures included requiring a six-
21 digit passcode to ensure that Mr. Terpin’s account would not readily be hacked,
22 including by someone spoofing his identity and attempting to transfer his telephone
23 number to their phone. In fact, AT&T’s representations were false because an
24 imposter was readily able to obtain Mr. Terpin’s wireless number from a
25 cooperative (or wantonly incompetent) employee at an AT&T facility on January 7,
26 2018 without having either proper identification or being asked to provide the
27 required six-digit passcode.
28

1 128. Even without AT&T's misrepresentations after the June 11,
2 2017 hack, Mr. Terpin was entitled to assume that AT&T would take appropriate
3 measures to keep secure his Personal Information, including CPI and CPNI,
4 because of its statements in its Privacy Policy and COBC. AT&T did not disclose
5 at any time that Mr. Terpin's CPI and CPNI were vulnerable to hackers because
6 AT&T's security measures were ineffective. AT&T, which was the only party in
7 possession of material information as to its own practices, did not disclose the
8 rampant defects in its security procedures, including the ability of its employees to
9 bypass such procedures, when it had a duty to do so. AT&T further violated the
10 UCL by failing to implement reasonable and appropriate security measures for Mr.
11 Terpin's Personal Information, as required by the FCA, the CPNI Rules, the
12 Consent Decree and California law, or following industry standards for data
13 security, and failing to comply with its own Privacy Policy and COBC. If AT&T
14 had complied with these legal requirements, Mr. Terpin would not have suffered
15 the damages related to the January 7, 2018 SIM swap fraud.

16 129. AT&T's acts, omissions, and misrepresentations as alleged
17 herein were unlawful and in violation of, *inter alia*, the FCA, 47 U.S.C. §§ 206 and
18 222, the CPNI Rules, the Consent Decree, Cal. Civ. Code § 1798.81.5(b), Section
19 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), Cal. Bus. & Prof.
20 Code § 22576 (because of AT&T failing to comply with its own posted privacy
21 policies), and the Consumer Legal Remedies Act, Cal. Civ. Code § 1750 *et seq.*

22 130. Mr. Terpin suffered injury in fact and loss money or property,
23 including stolen crypto currencies worth nearly \$24 million, as the result of
24 AT&T's unlawful business practices. Mr. Terpin has lost the benefit of his bargain
25 for his purchased services from AT&T that he would not have paid if he had known
26 the truth regarding AT&T's inadequate data security.

131. Because of AT&T's unlawful business practices and violation of the UCL, Mr. Terpin is entitled to restitution, disgorgement of wrongfully obtained profits, and injunctive relief.

FIFTH CLAIM FOR RELIEF
(Violation of California Unfair Competition Law
Unfair Business Practice
Cal. Bus. & Prof. Code § 17200 *et seq.*)

132. Plaintiff realleges the allegations in Paragraphs 1-131 as if fully stated herein.

133. Because of the conduct alleged herein, AT&T engaged in unfair business practices within the meaning of the UCL.

134. AT&T stored and processed Mr. Terpin's Personal Information, including CPI and CPNI, in its electronic system and databases. Mr. Terpin's Personal Information was readily accessed when a hacker through SIM swap fraud gained access to Mr. Terpin's telephone number. AT&T represented to Mr. Terpin through its Privacy Policy and COBC that its systems and databases were secure and that his Personal Information would remain private and secure and would not be divulged to unauthorized third parties. AT&T engaged in unfair acts and business practices by representing in its Privacy Policy that it had "established electronic and administrative safeguards designed to make the information we collect secure." AT&T further represented that all its employees followed the COBC and that such employees "must follow the laws, rules, regulations, court and/or administrative orders that apply to our business—including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of your [i.e., the customer's] records."

135. AT&T further assured Mr. Terpin, after the June 11, 2017 hack, that his Personal Information, including CPI and CPNI, was secure because AT&T

1 had implemented additional security protections on his account, which it called a
2 “higher security level” or “special”, “high risk,” or “celebrity” protection.

3 136. Even without these misrepresentations, Mr. Terpin was entitled
4 to, and did, assume AT&T would take appropriate measures to keep his Personal
5 Information safe under the FCA, the CPNI Rules, the Consent Decree and other
6 laws and regulations. AT&T did not disclose at any time that Mr. Terpin’s
7 Personal Information was vulnerable to hackers by employees’ turning over his
8 telephone number that included and allowed access to his Personal Information.
9 AT&T also did not disclose that its security measures were inadequate and
10 outdated, its employees were not properly trained, that its employees could readily
11 bypass its security procedures, and that it did not properly vet its employees to
12 ensure that they were ethical and did not have a criminal record.

13 137. AT&T knew or should have known that it did not employ
14 reasonable security and lacked adequate employee training and monitoring
15 measures that would have kept Mr. Terpin’s personal and financial information
16 secure and prevented the loss or misuse of Mr. Terpin’s Personal information.
17 AT&T had been put on notice through the Consent Decree and by the June 11,
18 2017 hack of its lax security practices and inadequate training and supervision of
19 employees. AT&T’s system is less secure than the access portals for numerous
20 gyms, which require fingerprint identification for entrance.

21 138. AT&T violated the UCL by misrepresenting, both by
22 affirmative conduct and by omission, the security of its systems and services, and
23 its ability to safeguard Mr. Terpin’s Personal Information, including CPI and CPNI.
24 AT&T also violated the UCL by failing to implement and maintain reasonable
25 security procedures and practices appropriate to protect Mr. Terpin’s Personal
26 Information under the FCA, CPNI Rules, and Consent Decree, including CPI and
27 CPNI. If AT&T had followed the industry standards and legal requirements, Mr.
28 Terpin would not have suffered the damages related to the January 7, 2018 SIM

1 swap fraud. Moreover, if AT&T had followed the higher security measures it
2 purportedly employed after the June 11, 2017 hack, Mr. Terpin would not have
3 suffered the damages from the January 7, 2018 SIM swap fraud.

4 139. AT&T also violated its commitment to maintain the
5 confidentiality and security of Mr. Terpin's Personal Information, including CPI
6 and CPNI, and failed to comply with its own policies and applicable laws,
7 regulations, including the FCA, CPNI Rules, and the Consent Decree, and industry
8 standards relating to data security.

9 140. The harm caused by AT&T's actions and omissions, as
10 described in detail in this Complaint, greatly outweighs any perceived utility.
11 Indeed, AT&T's failure to follow data security protocols, its own policies, and its
12 misrepresentations to Mr. Terpin had no utility at all.

13 141. AT&T's actions and omissions, as described above, violated
14 fundamental public policies expressed by the United States and California. *See*,
15 *e.g.*, FCA, 47 U.S.C. § 222; CPNI Rules; Consent Decree; Cal. Civ. Code § 1798.1
16 ("The [California] Legislature declares that . . . all individuals have a right of
17 privacy in information pertaining to them . . . The increasing use of computers . . .
18 has greatly magnified the potential risk to individual privacy that can occur from
19 the maintenance of personal information); Cal. Civ. Code § 1798.81.5(a) ("It is the
20 intent of the Legislature to ensure that personal information about California
21 residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the
22 Legislature that this chapter [including the Online Privacy Protection Act] is a
23 matter of statewide concern.) Defendants' acts and omission, and the injuries
24 caused by them, are thus "comparable to or the same as a violation of law. . ." *Cel-*
25 *Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.*, 20 Cal. 4th 163,
26 187 (1999).

27 142. The harm caused by AT&T's actions and omissions, as
28 described in detail above, is substantial in that it has caused Mr. Terpin to suffer

1 nearly \$24 million in actual financial harm because of AT&T’s unfair business
2 practices.

3 143. Because of AT&T’s unfair business practices and violations of
4 the UCL, Mr. Terpin is entitled to restitution, disgorgement of wrongfully obtained
5 profits and injunctive relief.

6 **SIXTH CLAIM FOR RELIEF**

7 **(Violation of California Unfair Competition Law**

8 **Fraudulent Business Practice**

9 **Cal. Bus. & Prof. Code § 17200, *et seq.*)**

10 144. Mr. Terpin realleges the allegations of Paragraphs 1-143 as if
11 fully set forth herein.

12 145. Because of the conduct alleged herein, AT&T engaged in
13 fraudulent business practices within the meaning of the UCL.

14 146. AT&T affirmatively represented to Mr. Terpin that his Personal
15 Information, including CPI and CPNI, was secure and that it would remain private.
16 AT&T engaged in fraudulent acts and business practices by misleadingly
17 misrepresenting in its Privacy Policy that it “worked hard to protect your
18 information” and had “established electronic and administrative safeguards
19 designed to make the information we collect secure.” AT&T further
20 misrepresented that these safeguards included making employees subject to the
21 COBC so that they had to “follow the laws, rules, regulations, court and/or
22 administrative orders that apply to our business—including, specifically, the legal
23 requirements and company policies surrounding the privacy of your records.”
24 COBC. AT&T also misrepresented that it took protecting the security of its
25 customers’ Personal Information “seriously” and that employees violating the
26 COBC were “subject to disciplinary action,” including dismissal. *Id.*

27 147. AT&T’s misrepresentations and fraudulent conduct were
28 particularly egregious because AT&T was subject to the Consent Decree that

1 required it, in the light of numerous violations by its employees of their obligation
2 to protect customers' Personal Information, including CPNI, to strengthen the
3 training and supervision of its employees.

4 148. AT&T further misrepresented in the COBC that it had
5 "implemented technology and security features and strict policy guidelines to
6 safeguard the privacy of your Personal Information" that included limiting access to
7 Personal Information and requiring authentication before providing Account
8 Information to authorized individuals. After the June 11, 2017 hack, AT&T also
9 misrepresented to Mr. Terpin it was placing a higher level of security protection on
10 the Personal Information of his "high risk" or "celebrity" account so that a six-digit
11 code was required to modify his account, including transferring his telephone
12 number to another phone.

13 149. AT&T not only made affirmative misrepresentations, but also
14 made fraudulent omissions by concealing the true facts from Mr. Terpin. AT&T
15 did not disclose to Mr. Terpin that its data security measures were woefully
16 substandard, that its employees could bypass its security measures, and that it did
17 not adequately supervise or monitor its employees so that they would adhere to the
18 commitments it made in the Privacy Policy and the COBC, as well as the
19 requirements of the FCA, CPNI Rules and Consent Decree.

20 150. AT&T's representations that it would secure the Personal
21 Information of Mr. Terpin were facts that reasonable persons could be expected to
22 rely upon when deciding whether to use (or continue to use) AT&T's services.

23 151. Mr. Terpin relied upon the representations that AT&T made
24 after the June 11, 2017 hack and in the Privacy Policy and COBC. Based on the
25 representations that AT&T was implementing a higher level of security, Mr. Terpin
26 was entitled to, and did, assume AT&T would take appropriate measures to keep
27 his Personal Information safe, including not handing over his wireless number that
28 would allow thieves to access such information. AT&T did not disclose that the

1 higher level of security was ineffective, and that Mr. Terpin's Personal Information
2 was vulnerable to hackers because AT&T did not follow its own procedures or
3 monitor its employees' implementation of the procedures, as required by the FCA,
4 CPNI Rules, and the Consent Decree.

5 152. Had Mr. Terpin known that AT&T's "heightened security" was
6 ineffective and that its representations about such security were false and he had
7 known that AT&T failed to disclose to him that its data security practices were
8 substandard and ineffective, he would not have continued to provide his Personal
9 Information to AT&T and continued their services.

10 153. Mr. Terpin suffered injury and lost money when AT&T ported
11 over his wireless telephone number to a hacker's phone that allowed the hacker to
12 steal nearly \$24 million worth of cryptocurrency.

13 154. Because of AT&T's fraudulent business practices and violations
14 of the UCL, Mr. Terpin is entitled to restitution, disgorgement of wrongfully
15 obtained profits and injunctive relief.

16 **SEVENTH CLAIM FOR RELIEF**

17 **(Violation of California Consumer Legal Remedies Act ("CLRA"))**

18 **Cal. Civ. Code § 1750 *et seq.*)**

19 155. Mr. Terpin realleges the allegations of Paragraphs 1 through 154
20 as if fully set forth herein.

21 156. The CLRA was enacted to protect consumers against unfair and
22 deceptive business practices. It extends to transactions that are intended to result,
23 or which have resulted, in the sale of goods or services to consumers. AT&T is
24 subject to the CLRA because it provided paid wireless services to Mr. Terpin and
25 AT&T's acts, omissions, representations and practices fall within the CLRA.

26 157. Mr. Terpin is a consumer within the meaning of Cal. Civ. Code
27 § 1761(d).
28

158. AT&T's acts, omissions, misrepresentations, and practices were and are likely to deceive consumers. By misrepresenting the safety and security of its protection of Personal Information, including CPI and CPNI, AT&T violated the CLRA. AT&T had exclusive knowledge of undisclosed material facts, namely, that its protection of Personal Information was defective, and withheld that information from Mr. Terpin.

159. AT&T's acts, omissions and practices alleged herein violated the CLRA, which provides, in relevant part, that: "(a) The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer are unlawful . . . ; (5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have . . . ; (7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another. . . ; (14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law. . . ; (16) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not."

160. AT&T stored and processed Mr. Terpin's Personal Information, including CPI and CPNI, on its systems and databases. AT&T represented to Mr. Terpin that his Personal Information was secure and would remain private. AT&T engaged in deceptive acts and business practices by the statements that it made in the Privacy Policy and COBC that users' Personal Information was secure and that it adhered to its legal obligations to protect Personal Information, including under the FCA, CPNI Rules and the Consent Decree.

161. AT&T knew or should have known that it did not employ reasonable measures to keep Mr. Terpin's Personal Information secure and prevent the loss or misuse of that information. In fact, AT&T did not adhere to its legal

1 obligations to protect Personal Information, including those under the FCA, CPNI
2 Rules and the Consent Decree.

3 162. AT&T's deceptive acts and business practices, including the
4 commitment it made after the June 11, 2017 hack to implement a higher level of
5 security for Mr. Terpin's Personal Information and account, induced Mr. Terpin to
6 entrust AT&T with his Personal Information and continue to subscribe to its
7 wireless services. But for AT&T's deceptive acts and business practices, Mr.
8 Terpin would not have continued to provide AT&T with its Personal Information
9 and continue to subscribe to its wireless services.

10 163. Mr. Terpin was harmed as the result of AT&T's violations of
11 the CLRA because his Personal Information was compromised by divulging it to
12 hackers without his consent which led to the loss of nearly \$24 million worth of
13 cryptocurrency through the January 7, 2018 SIM swap fraud.

14 164. Because of AT&T's violation of the CLRA, Mr. Terpin is
15 entitled to compensatory and exemplary damages, an order enjoining AT&T from
16 continuing the unlawful practices described herein, a declaration that AT&T's
17 conduct violated the CLRA, attorneys' fees, and the costs of litigation.

18 **EIGHTH CLAIM FOR RELIEF**

19 **(Deceit by Concealment—Cal. Civ. Code §§ 1709, 1710)**

20 165. Mr. Terpin realleges the allegations of Paragraphs 1-164 as if
21 fully set forth herein.

22 166. As alleged above, AT&T knew that its data security measures
23 were grossly inadequate, that its employees could readily bypass the procedures,
24 that its employees actively cooperated with hackers and thieves, and that it was
25 incapable of living up to its commitments to consumers, including to Mr. Terpin,
26 under state and federal law, as well as under its own Privacy Policy, to protect his
27 Personal Information, including CPI and CPNI.
28

1 167. As further alleged above, AT&T knew from prior incidents and
2 contacts with law enforcement that its system was subject to SIM swap fraud, that
3 its employees cooperated with hackers in such fraud, and that such fraud was
4 prevalent in the cryptocurrency community.

5 168. In response to these facts, AT&T chose to do nothing to protect
6 Mr. Terpin.

7 169. AT&T had an obligation to disclose to Mr. Terpin that his
8 Personal Information, including CPI and CPNI, was readily obtained by hackers
9 and that its own employees handed such information to hackers, and yet did not
10 implement measures to protect Mr. Terpin or willfully failed to adhere to any
11 measures that were in place, including its so-called “higher security level” for high
12 profile or celebrity accounts and its required security and training measures under
13 the Consent Decree. AT&T’s so-called security system more resembles a thin slice
14 of swiss cheese than a sophisticated network of “heightened security.”

15 170. AT&T did not disclose these things to Mr. Terpin and willfully
16 deceived Mr. Terpin by concealing the true facts concerning its data security, which
17 AT&T was legally obligated and had a duty to disclose. It is far easier to penetrate
18 AT&T’s system than obtaining a new password from Walmart.

19 171. Had AT&T disclosed the true facts about its dangerously poor
20 data security practices and its inadequate supervision and training of its employees,
21 Mr. Terpin would have taken further measures to protect himself. Mr. Terpin
22 justifiably relied on AT&T’s statements, including statements after the June 11,
23 2017 hack, and further relied on AT&T to provide accurate and complete
24 information about its data security.

25 172. Rather than disclosing the inadequacies in its security, AT&T
26 willfully suppressed any information relating to such inadequacies.

27 173. AT&T’s actions are “deceit” under Cal. Civ. Code § 1710 in
28 that they are the suppression of a fact by one who is bound to disclose it, or who

1 gives information of other facts which are likely to mislead for want of
2 communication of that fact.

3 174. Because of the deceit by AT&T, it is liable under Cal. Civ. Code
4 § 1709 for “any damage which [Mr. Terpin] thereby suffers.”

5 175. Because of this deceit by Defendants, Mr. Terpin’s Personal
6 Information, including his CPI and CPNI, was compromised by hackers and he was
7 deprived of nearly \$24 million worth of cryptocurrency. In addition, Mr. Terpin’s
8 Personal Information is now easily available to hackers, including through the Dark
9 Web. Mr. Terpin is further damaged to the extent of the amounts that he has paid
10 AT&T for wireless services, because those services were either worth nothing or
11 worth less than was paid for them because of lack of security. Mr. Terpin has also
12 suffered substantial out-of-pocket costs because of AT&T’s inadequate security.

13 176. Because AT&T’s deceit is fraud under Civil Code § 3294(c)(3),
14 and AT&T’s conduct was done with malice, fraud and oppression, Mr. Terpin is
15 entitled to punitive damages under Civil Code § 3294(a).

16 **NINTH CLAIM FOR RELIEF**

17 **(Misrepresentation)**

18 177. Mr. Terpin realleges Paragraphs 1 through 176 as if fully set
19 forth herein.

20 178. As outlined above, AT&T made numerous representations and
21 false promises in its Privacy Policies and COBC as well as in its advertising,
22 regarding the supposed security of consumers’ Personal Information, including Mr.
23 Terpin’s Personal Information, and when an AT&T employee persuaded Mr.
24 Terpin not to cancel his service after the June 11, 2017 hack. Such representations
25 and promises were false because AT&T was using outdated security procedures and
26 failed to disclose that it did not adhere to its own standards, including the
27 heightened security standards that it implemented for Mr. Terpin after the June 11,
28 2017 hack, the CPNI Rules or the procedures mandated by the Consent Decree.

1 179. AT&T's misrepresentations and false promises, including those
2 made after the June 11, 2017 hack, were material to Mr. Terpin who reasonably
3 relied upon the representations and promises. Mr. Terpin would not have agreed to
4 continue to use and pay for AT&T's services if he had known that they were not as
5 secure as represented by AT&T and would not have lost nearly \$24 million.

6 180. AT&T intended that Mr. Terpin rely on their representations and
7 promises, including those made after the June 11, 2017 hack, as it knew that Mr.
8 Terpin would not entrust his Personal Information to unreasonable security risks,
9 particularly because Mr. Terpin had been subject to the June 11, 2017 hack. In
10 reliance upon AT&T's representations and promises, Mr. Terpin continued to
11 maintain a wireless account with AT&T and to use his AT&T phone number for
12 verification and other purposes.

13 181. As a direct and proximate result of AT&T's wrongful actions,
14 Mr. Terpin has been damaged by paying monthly fees to AT&T and having thieves
15 steal nearly \$24 million worth of cryptocurrency through the January 7, 2018 SIM
16 swap fraud.

17 182. AT&T's misconduct is fraud under Civil Code § 3294(c)(3) in
18 that it was deceit or concealment of a material fact known to AT&T conducted with
19 the intent on the part of AT&T of depriving Mr. Terpin of legal rights or otherwise
20 causing injury. AT&T's conduct was done with malice, fraud or oppression under
21 Civil Code § 3294(c)(1) and (2) and Mr. Terpin is entitled to punitive damages
22 against AT&T under Civil Code §3294(a).

23 **TENTH CLAIM FOR RELIEF**

24 **(Negligence)**

25 183. Plaintiff realleges the allegations in Paragraphs 1 through 182 as
26 if fully set forth herein.

27 184. AT&T owed a duty to Mr. Terpin to exercise reasonable care in
28 safeguarding and protecting his Personal Information, including CPI and CPNI, and

1 keeping it from being compromised, lost, stolen, misused and/or disclosed to
2 unauthorized parties. This duty included, among other things, designing,
3 maintaining, and testing its security systems to ensure that Mr. Terpin's Personal
4 Information, including CPI and CPNI, was adequately secured and protected.
5 AT&T had a further duty to implement and adhere to the "high security" or
6 "celebrity" protocol that it had promised Mr. Terpin that it would place on his
7 account to protect his Personal Information and had a duty to adhere to the FCA,
8 CPNI Rules, and the provisions of the Consent Decree.

9 185. AT&T knew that Mr. Terpin's Personal Information, including
10 CPI and CPNI, was confidential and sensitive. Indeed, AT&T acknowledged this
11 in its Privacy Policy and in agreeing, at Mr. Terpin's request, to place additional
12 "high security" measures on Mr. Terpin's account to prevent hackers from
13 committing SIM swap fraud on Mr. Terpin. AT&T further promoted its "extra
14 security" on its website. AT&T likewise knew that Mr. Terpin's Personal
15 Information was vulnerable to hacks by thieves and other criminals both because it
16 acknowledged such in its Privacy Policy and because it had been informed by Mr.
17 Terpin of the June 11, 2017 hack. AT&T thus knew of the substantial harms that
18 could occur to Mr. Terpin if it did not place adequate security on his Personal
19 Information and did not follow its own "high security" measures for the account.

20 186. By being entrusted by Mr. Terpin to safeguard his Personal
21 Information, including CPI and CPNI, AT&T had a special relationship with Mr.
22 Terpin. Mr. Terpin signed up for AT&T's wireless services and agreed to provide
23 his Personal Information to AT&T with the understanding that AT&T would take
24 appropriate measures to protect it. But AT&T did not protect Mr. Terpin's
25 Personal Information and violated his trust. AT&T knew its security was
26 inadequate in part due to the FCC investigation that led to the Consent Decree.
27 AT&T is morally culpable, given prior security breaches involving its own
28 employees.

187. AT&T breached its duty to exercise reasonable care in safeguarding and protecting Mr. Terpin's Personal Information, including CPI and CPNI, by failing to adopt, implement, and maintain adequate security measures to safeguard that information, including its duty under the FCA, CPNI Rules, the Consent Decree, and its own Privacy Policy.

188. AT&T's failure to comply with federal and state requirements for security further evidences AT&T's negligence in failing to exercise reasonable care in safeguarding and protecting Mr. Terpin's Personal Information, including CPI and CPNI.

189. But for AT&T's wrongful and negligent breach of its duties owed to Mr. Terpin, his Personal Information, including his CPI and CPNI, would not have been compromised, stolen, viewed, and used by unauthorized persons. AT&T's negligence was a direct and legal cause of the theft of Mr. Terpin's Personal Information and the legal cause of his resulting damages, including, but not limited to, the theft of nearly \$24 million worth of cryptocurrency.

190. The injury and harm suffered by Mr. Terpin was the reasonably foreseeable result of AT&T's failure to exercise reasonable care in safeguarding and protecting Mr. Terpin's Personal Information, including his CPI and CPNI. The harm was additionally foreseeable in that AT&T was aware that Mr. Terpin was a holder and user of cryptocurrency and a potential victim of hacking following the June 11, 2017 hack.

191. AT&T's misconduct as alleged herein is malice, fraud or oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable conduct carried on by AT&T with a willful and conscious disregard of the rights or safety of Mr. Terpin and despicable conduct that has subjected Mr. Terpin to cruel and unjust hardship in conscious disregard of his rights. As a result, Mr. Terpin is entitled to punitive damages against AT&T under Civil Code § 3294(a).

ELEVENTH CLAIM FOR RELIEF

(Negligent Supervision and Training)

192. Mr. Terpin realleges the allegations of Paragraphs 1 through 191 as if fully set forth herein.

193. AT&T owed a duty to Mr. Terpin to exercise reasonable care in supervising and training its employees to safeguard and protect his Personal Information, including CPI and CPNI, and to keep it from being compromised, lost, stolen, misused and/or disclosed to unauthorized parties. This duty included AT&T's instructing its employees to adhere to the "high security" or "extra security" protocols that AT&T had promised Mr. Terpin it would place on his account to protect his Personal Information.

194. AT&T was aware of the ability of its employees to bypass its security measures and the fact that its employees actively participated in fraud involving its customers, including pretexting and SIM card swap fraud, by bypassing such security measures.

195. AT&T knew that Mr. Terpin's Personal Information, including CPI and CPNI, was confidential and sensitive. AT&T further knew that Mr. Terpin's Personal Information was vulnerable to hacks and SIM swap fraud by thieves and other criminals because it had been informed by Mr. Terpin of the June 11, 2017 hack.

196. By being entrusted by Mr. Terpin to safeguard his Personal Information, including CPI and CPNI, AT&T had a special relationship with Mr. Terpin. Mr. Terpin signed up for AT&T's wireless services and agreed to provide his Personal Information to AT&T with the understanding that AT&T's employees would take appropriate measures to protect it. AT&T also made promises in the COBC that its employees would respect its customers' privacy and was further required by the Consent Decree to supervise and train its employees to adhere to its legal obligations to protect their Personal Information.

1 197. AT&T breached its duty to supervise and train its employees to
2 safeguard and protect Mr. Terpin's Personal Information, including CPI and CPNI,
3 by not requiring them to adhere to its obligations under the CPNI Rules, the
4 Consent Decree and other legal provisions. On January 7, 2018, AT&T's
5 employees facilitated SIM swap fraud on Mr. Terpin by not requiring individuals
6 requesting Mr. Terpin's telephone number to present valid identification. AT&T
7 employees also failed to follow AT&T's "higher" or "extra" security by not
8 requiring the individual requesting Mr. Terpin's telephone number to provide the
9 secret six-digit code that AT&T had given Mr. Terpin to prevent precisely such
10 fraud.

11 198. AT&T knew its supervision and monitoring of its employees
12 was inadequate through: a) the FCC investigation that led to the Consent Decree
13 mandating measures to improve such training and monitoring; and b) its knowledge
14 from prior incidents that its employees cooperated with hackers in SIM swap fraud.
15 AT&T is morally culpable, given prior security breaches involving its own
16 employees.

17 199. AT&T breached its duty to exercise reasonable care in
18 supervising and monitoring its employees to protect Mr. Terpin's Personal
19 Information, including CPI and CPNI.

20 200. AT&T's failure to comply with the Consent Decree and to
21 follow the requirements of the FCA and CPNI Rules further evidence AT&T's
22 negligence in adequately supervising and monitoring its employees so that they
23 would safeguard and protect Mr. Terpin's Personal Information, including CPI and
24 CPNI.

25 201. But for AT&T's wrongful and negligent breach of its duties to
26 supervise and monitor its employees, Mr. Terpin's CPI and CPNI would not have
27 been disclosed to unauthorized individuals through SIM swap fraud. AT&T's
28 negligence was a direct and legal cause of the theft of Mr. Terpin's Personal

1 Information and the legal cause of his resulting damages, including, but not limited
2 to, the theft of nearly \$24 million worth of cryptocurrency.

3 202. The injury and harm suffered by Mr. Terpin was the reasonably
4 foreseeable result of AT&T's failure to supervise and monitor its employees in
5 safeguarding and protecting Mr. Terpin's Personal Information, including his CPI
6 and CPNI.

7 203. AT&T's misconduct as alleged here is done with malice, fraud
8 and oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable
9 conduct carried on by AT&T with a willful and conscious disregard of the rights or
10 safety of Mr. Terpin and despicable conduct that has subjected Mr. Terpin to cruel
11 and unjust hardship in conscious disregard of his rights. As a result, Mr. Terpin is
12 entitled to punitive damages against AT&T under Civil Code § 3294(a).

13 **TWELFTH CLAIM FOR RELIEF**

14 **(Negligent Hiring)**

15 204. Mr. Terpin realleges the allegations in Paragraphs 1 through 203
16 as if fully set forth herein.

17 205. AT&T owed a duty to Mr. Terpin to exercise reasonable care in
18 hiring competent, honest, and ethical employees to safeguard and protect his
19 Personal Information, including CPI and CPNI, to keep it from being compromised,
20 lost, stole, misused and/or disclosed to unauthorized parties. AT&T also owed a
21 duty to exercise reasonable care in the operation of AT&T stores, including by third
22 parties, and their hiring of employees for those AT&T stores.

23 206. AT&T knew that Mr. Terpin's Personal Information, including
24 CPI and CPNI, was confidential and sensitive. AT&T further knew that Mr.
25 Terpin's Personal Information was vulnerable to hacks and SIM swap fraud by
26 thieves and other criminals because it had been informed by Mr. Terpin of the June
27 11, 2017 hack. AT&T further knew from the investigation that led to the Consent
28 Decree that its employees had cooperated with hackers and thieves by turning over

1 to them the CPNI of its customers to facilitate fraud and theft. It also knew from
2 prior incidents of SIM swap fraud that its employees cooperated with hackers and
3 thieves defrauding AT&T's own customers.

4 207. By being entrusted by Mr. Terpin to safeguard his Personal
5 Information, including CPI and CPNI, AT&T had a special relationship with Mr.
6 Terpin. Mr. Terpin signed up for AT&T's wireless services and agreed to provide
7 his Personal Information to AT&T with the understanding that AT&T's employees
8 would take appropriate measures to protect it. AT&T also made promises in the
9 COBC that its employees would adhere to AT&T's ethical and legal obligations,
10 including respecting its customers' privacy. AT&T was further required by the
11 Consent Decree to correct the practices that had led to hiring employees who had
12 cooperated with hackers and thieves and stolen customers' personal information.

13 208. AT&T breached its duty to hire employees who would
14 safeguard and protect Mr. Terpin's Personal Information, including CPI and CPNI.
15 Mr. Terpin alleges on information and belief, that the employees who facilitated the
16 SIM swap fraud perpetrated on Mr. Terpin did not live up to AT&T's purported
17 ethical standards, as expressed in the COBC, or to their legal obligations to Mr.
18 Terpin. Mr. Terpin further alleges on information and belief, that the employee at
19 the AT&T store who ported Mr. Terpin's telephone number to the hackers on
20 January 7, 2018, had a criminal record and colluded with the hackers in perpetrating
21 the fraud on Mr. Terpin.

22 209. AT&T knew that its hiring of employees was inadequate
23 through the FCC investigation that led to the Consent Decree that revealed that
24 employees had actively handed over the Personal Information of its customers to
25 hackers and thieves. AT&T is morally culpable, given the prior conduct of its
26 employees.

1 210. AT&T breached its duty to properly hire competent, honest and
2 ethical employees to protect Mr. Terpin's Personal Information, including CPI and
3 CPNI.

4 211. AT&T's failure to comply with the Consent Decree is further
5 evidence of its failure to investigate employees to ensure that they adhered to
6 AT&T's ethical and legal responsibilities.

7 212. On information and belief, the employee at the AT&T store who
8 gave Mr. Terpin's SIM card to the imposter on January 7, 2018 was Jahmil Smith.
9 Smith has a criminal record which AT&T should have discovered before or after
10 hiring him.

11 213. But for AT&T's wrongful and negligent breach of its duties to
12 hire ethical and competent employees, Mr. Terpin's CPI and CPNI would not have
13 been disclosed to unauthorized individuals through SIM swap fraud. AT&T's
14 negligence was a direct and legal cause of the theft of Mr. Terpin's Personal
15 Information and the legal cause of his resulting damages, including, but not limited
16 to, the theft of nearly \$24 million worth of cryptocurrency.

17 214. The injury and harm suffered by Mr. Terpin was the reasonably
18 foreseeable result of AT&T's failure to hire competent and ethical employees who
19 would safeguard and protect Mr. Terpin's Personal Information, including his CPI
20 and CPNI. Indeed, this failure on the part of AT&T led to the January 7, 2018 SIM
21 swap fraud.

22 215. AT&T's misconduct as alleged herein is malice, fraud and
23 oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable conduct
24 carried on by AT&T with a willful and conscious disregard of the rights or safety of
25 Mr. Terpin and despicable conduct that has subjected Mr. Terpin to cruel and unjust
26 hardship in conscious disregard of his rights. As a result, Mr. Terpin is entitled to
27 punitive damages against AT&T under Civil Code § 3294(a).
28

THIRTEENTH CLAIM FOR RELIEF

(Breach of Contract – Privacy Policy)

216. Mr. Terpin realleges the allegations in Paragraphs 1 through 215 as if fully set forth herein.

217. The Privacy Policy is a binding contract between AT&T and Mr. Terpin.

218. AT&T breached the contract with respect to at least the following provisions of the Privacy Policy:

- AT&T’s promise that it will not sell or disclose users’ “Personal Information” to anyone;
- AT&T’s commitments that it has “worked hard to protect your information” and has “established electronic and administrative safeguards designed to make the information we collect secure”;
- AT&T’s promise that its employees must follow its COBC and that “all employees must follow the laws, rules, regulations, court and/or administrative orders that apply to our business—including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of your records”;
- AT&T’s promise that it subjects employees who do not meet its security standards to “disciplinary action” and dismissal;
- AT&T’s promise that it has “implemented technology and security features and strict policy guidelines to safeguard the privacy of your Personal Information”;
- AT&Ts promise that it “maintain[s] and protect[s] the security of computer storage and network equipment”;

- AT&T commitment that it limits access to Personal Information “to only those with jobs requiring such access”; and
- AT&T’s promise that it “[r]equire[s] caller/online authentication before providing Account Information so that only you or someone who knows your Account Information will be able to access or change this information.”

219. AT&T also breached its COBC by failing to follow “not only the letter of the law, but the spirit of the law” and failing to “protect the privacy of our customers’ communications because “not only do our customers demand this, but the law requires it.”

220. AT&T breached these provisions of its Privacy Policy and COBC by not having proper safeguards in accordance with law, including the FCA, CPNI Rules, and the Consent Decree, and Cal. Civ. Code §1798.81.5, to protect Mr. Terpin’s “Personal Information,” including CPI and CPNI. AT&T further breached its promises by not limiting access to Mr. Terpin’s Personal Information to authorized or properly trained individuals. AT&T likewise violated its commitments to maintain the confidentiality and security of Mr. Terpin’s Personal Information by failing to comply with its own policies and applicable “law, rules, regulations, court and/or administrative orders that apply to our business—including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of your records.” AT&T thus breached its obligations under the FCA, CPNI Rules, the Consent Decree and California law.

221. The January 7, 2018 SIM swap fraud was a direct and legal cause of the injuries and damages suffered by Mr. Terpin, including loss of nearly \$24 million of crypto currency.

222. To the extent that AT&T maintains that the Exculpatory Provision, Damages Restriction, and the Indemnity in the Agreement apply to the promises made by AT&T in the Privacy Policy and the COBC, such provisions, as well as the Agreement in its entirety, are unenforceable and do not apply to the Privacy Policy and COBC. *See* Cal. Civ. Code §§1670.5, 1668 (contracts are unenforceable if unconscionable or void against public policy); *Ingle v. Circuit City Stores, Inc.*, 328 F.3d 1165, 1180 (9th Cir. 2003) (contracts void if central purpose is tainted with illegality). Moreover, such provisions are unconscionable under California law because an entity cannot exculpate itself from its obligations to maintain the privacy and security of personal information under federal and California law, as further set forth herein in Paragraphs 70 to 82. *See Health Net of California, Inc. v. Department of Health Services*, 113 Cal. App. 4th 224, 244 (2004) (California courts for 85 years have invalidated “contract clauses that relieve a party from responsibility for future statutory and regulatory violations”)

223. Mr. Terpin was harmed due to AT&T’s breach of the terms of the Privacy Policy and COBC, because his “Personal Information,” including CPI and CPNI, was breached in the January 7, 2018 SIM swap fraud, which led to monetary losses of nearly \$24 million.

FOURTEENTH CLAIM FOR RELIEF

(Breach of Implied Contracts

In the Alternative to Claim for Breach of Express Contract)

224. Mr. Terpin realleges the allegations of Paragraphs 1 through 223 as if fully set forth herein.

225. To the extent that AT&T’s Privacy Policy and COBC did not form express contracts, the opening of an AT&T wireless account by Mr. Terpin created implied contracts between AT&T and Mr. Terpin as to the protection of his Personal Information, the terms of which were set forth by the relevant Privacy Policy and COBC.

1 226. AT&T breached such implied contracts by failing to adhere to
2 the terms of the applicable Privacy Policy and COBC, as described above in Mr.
3 Terpin's Thirteenth Claim for Relief. AT&T violated its commitment to maintain
4 the confidentiality and security of the Personal Information of Mr. Terpin, including
5 CPI and CPNI, and failed to comply with its own policies and "laws, rules,
6 regulations, court and/or administrative orders that apply to [AT&T's] business—
7 including, specifically, the privacy of communications and the security and privacy
8 of your records." COBC.

9 227. Mr. Terpin was harmed because of AT&T's breach of the terms
10 of the Privacy Policy and COBC, because his "Personal Information," including
11 CPI and CPNI, were breached in the January 7, 2018 SIM swap fraud, which led to
12 monetary losses of nearly \$24 million.

13 **FIFTEENTH CLAIM FOR RELIEF**

14 **(Breach of the Covenant of Good Faith and Fair Dealing)**

15 228. Mr. Terpin realleges the allegations of Paragraphs 1 through 227
16 as if fully set forth herein.

17 229. Under California law, there is an implied covenant of good faith
18 and fair dealing in every contract that neither party will do anything which will
19 injure the right of the other to receive the benefits of the agreement.

20 230. Under the express and implied terms of the relationship between
21 Mr. Terpin and AT&T, including through the Privacy Policy and COBC, Mr.
22 Terpin and AT&T were to benefit using AT&T's services, while AT&T was
23 supposed to benefit through money received for Mr. Terpin subscribing to AT&T's
24 wireless services.

25 231. AT&T exhibited bad faith through its conscious awareness of
26 and deliberate indifference to the risk to Mr. Terpin's Personal Information,
27 including CPI and CPNI, by (a) not implementing security measures adequate to
28 protect his Personal Information; (b) improperly hiring, training and supervising its

1 employees; (c) not adhering to its own security standards, including the “high
2 security” standards for “high profile” or “celebrity” account holders; and (d) failing
3 to invest in adequate security protections.

4 232. AT&T, by exposing Mr. Terpin to vastly greater security risks,
5 breached its implied covenant of good faith and fair dealing with respect to the
6 terms of its Privacy Policy and COBC and the implied warranties of their
7 contractual relationship with their users.

8 233. Mr. Terpin was harmed because of AT&T’s breach of the
9 implied covenant of good faith and fair dealing because his Personal Information
10 was compromised by the hackers in the January 7, 2018 SIM swap fraud which led
11 to monetary damages of nearly \$24 million.

12 234. AT&T’s misconduct as alleged herein is fraud under Civil Code
13 § 3294(c)(3) in that it was deceit or concealment of a material fact known to AT&T
14 conducted with an intent on the part of AT&T of depriving Mr. Terpin of “legal
15 rights or otherwise concerning injury.” In addition, AT&T’s misconduct, as alleged
16 herein, is malice, fraud or oppression under Civil Code § 3294(c)(1) and (2) in that
17 it was despicable conduct carried on by AT&T with a willful and conscious
18 disregard of the rights or safety of Mr. Terpin and has subjected Mr. Terpin to cruel
19 and unjust hardship in conscious disregard of his rights. As a result, Mr. Terpin is
20 entitled to punitive damages against AT&T under Civil Code § 3294(a).

21 **SIXTEENTH CLAIM FOR RELIEF**

22 **(Violation of California’s Customer Records Act—Inadequate Security**

23 **Cal. Civ. Code § 1798.81.5)**

24 235. Mr. Terpin realleges the allegations of Paragraphs 1 through 234
25 as if fully set forth herein.

26 236. California Civil Code §1798.80 *et seq.*, known as the Customer
27 Records Act (“CRA”), was enacted to “encourage businesses that own, license, or
28

1 maintain personal information about Californians to provide reasonable security for
2 that information.” Civil Code § 1798.81.5(a)(1).

3 237. Civil Code § 1798.81.5(b) requires any business that “owns,
4 licenses or maintains personal information about a California resident” to
5 “implement and maintain reasonable security procedures and practices appropriate
6 to the nature of the information” and “to protect the personal information from
7 unauthorized access, destruction, use, modification or disclosure.” Civil Code §
8 1798.81.5(d)(1)(B) defines “personal information” as including account numbers,
9 passwords and other sensitive information relating to individuals.

10 238. AT&T is a business that owns, licenses, or maintains the
11 personal information of California residents. As alleged herein, AT&T did not
12 “implement and maintain reasonable security procedures and practices” regarding
13 Personal Information and protect it “from unauthorized access, destruction, use,
14 modification or disclosure” as evidenced by the January 7, 2018 SIM swap fraud.

15 239. As a direct and legal result of AT&T’s violation of Civil Code §
16 1798.81.5, Mr. Terpin was harmed because disclosure of his wireless account
17 information allowed hackers to steal nearly \$24 million worth of cryptocurrency.

18 240. Mr. Terpin seeks remedies available under Cal. Civ. Code §
19 1798.84, including, but not limited to damages suffered by him as alleged above
20 and equitable relief.

21 241. AT&T’s conduct is fraud under Civil Code § 3294(c)(3) in that
22 it was deceit or concealment of a material fact known to AT&T conducted with the
23 intent of AT&T to deprive Mr. Terpin of his legal rights or otherwise causing
24 injury. Because the misconduct was done with malice, fraud and oppression, Mr.
25 Terpin is entitled to punitive damages against AT&T under Civil Code § 3294(a).

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

PRAYER FOR RELIEF

Wherefore, Plaintiff Michael Terpin demands judgment against Defendants as follows:

1. For general damages against Defendants, and each of them, jointly and severally, in an amount to be determined at trial, but in no event less than \$24,000,000;

2. For exemplary and punitive damages against Defendants, and each of them, in an amount to be determined at trial, but in no event greater than nine times the amount of general and special damages awarded to Plaintiff (\$216 million);

3. For preliminary and permanent injunctive relief against Cross-Defendants, and each of them, enjoining and restraining them from continue to engage in unfair competition, unfair practices, violation of privacy, and other actions;

4. For a declaration that the Agreement in its entirety is unenforceable as unconscionable and against public policy or, in the alternative, that (a) the Exculpatory Provision is unenforceable as against Plaintiff; (b) the Damages Resolution is unenforceable against Plaintiff; and (c) the Indemnity is unenforceable against Mr. Terpin;

5. For attorney's fees under the FCA, California Penal Code § 202(e)(1), the California Legal Remedies Act and other applicable statutory provision;

6. For restitution, disgorgement of wrongfully obtained profits and injunctive relief pursuant to California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*;

7. For a declaration that AT&T's conduct violated the California Legal Remedies Act; and

1 8. For interest and costs of suit and such other and further relief as the
2 Court deems just and proper.

3 DATED: August 15, 2018

GREENBERG GLUSKER FIELDS
CLAMAN & MACHTINGER LLP

By: /s/Pierce O'Donnell

PIERCE O'DONNELL (SBN 081298)
Attorneys for Plaintiff Michael Terpin

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

DEMAND FOR JURY TRIAL

Plaintiff hereby requests a trial by jury.

DATED: August 15, 2018

GREENBERG GLUSKER FIELDS
CLAMAN & MACHTINGER LLP

By:/s/ Pierce O'Donnell

PIERCE O'DONNELL (SBN 081298)
Attorneys for Plaintiff Michael Terpin

GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590

EXHIBIT “A”

30 FCC Rcd. 2808 (F.C.C.), 30 F.C.C.R. 2808, 62 Communications Reg. (P&F) 526, 2015 WL 1577197

Federal Communications Commission (F.C.C.)
Order

IN THE MATTER OF AT&T SERVICES, INC.

File No.: EB-TCD-14-00016243

Acct. No.: 201532170010

FRN: 0005193701

DA 15-399

Released: April 8, 2015

Adopted: April 8, 2015

****1 *2808** By the Chief, Enforcement Bureau:

1. The Enforcement Bureau (Bureau) of the Federal Communications Commission (Commission) has entered into a Consent Decree to resolve its investigation into whether AT&T Services, Inc. (AT&T or Company) failed to properly protect the confidentiality of almost 280,000 customers' proprietary information, including sensitive personal information such as customers' names and at least the last four digits of their Social Security numbers, as well as account-related data known as customer proprietary network information (CPNI), in connection with data breaches at AT&T call centers in Mexico, Columbia, and the Philippines. At least two employees believed to have engaged in the unauthorized access confessed that they sold the information obtained from the breaches to a third party, known to them as "El Pelon." The breaches resulted in the personal information of 51,422 AT&T customers' information being used to place 290,803 handset unlock requests through AT&T's online customer unlock request portal. The investigation also examined whether AT&T promptly notified law enforcement authorities of the security breaches involving its customers' CPNI.

2. The failure to reasonably secure customers' proprietary information violates a carrier's statutory duty under the Communications Act to protect that information, and also constitutes an unjust and unreasonable practice in violation of the Act. These laws ensure that consumers can trust that carriers have taken appropriate steps to ensure that unauthorized persons are not accessing, viewing or misusing their personal information. The Commission has made clear that it expects telecommunications carriers such as AT&T to take "every reasonable precaution" to protect their customers' data, and that it is committed to protecting the personal information of American consumers from misappropriation, breach, and unlawful disclosure. In addition, the laws that require prompt disclosure of data breaches to law enforcement authorities, and subsequently to consumers, aid in the pursuit and apprehension of bad actors and provide valuable information that helps affected consumers be proactive in protecting themselves in the aftermath of a data breach. To settle this matter, AT&T will pay a civil penalty of \$25,000,000 and develop and implement a compliance plan to ensure appropriate processes and procedures are incorporated into AT&T's business practices to protect consumers against similar data breaches in the future. In particular, AT&T will be required to improve its privacy and data security practices by appointing a senior compliance manager who is privacy certified, conducting a privacy risk assessment, implementing an information security program, preparing an appropriate compliance manual, and regularly training employees on the company's privacy policies and the applicable privacy legal authorities.

****2** 3. After reviewing the terms of the Consent Decree and evaluating the facts before us, we find that the public interest would be served by adopting the Consent Decree and terminating the referenced investigation regarding AT&T's compliance with 201(b) and 222 of the Communications Act ***2809** of 1934, as amended (Communications Act or Act),¹ and Sections 64.2010(a) and 64.2011(b) of the Commission's Rules² in connection with a data breach.

4. In the absence of material new evidence relating to this matter, we conclude that our investigation raises no substantial or material questions of fact as to whether AT&T possesses the basic qualifications, including those related to character, to hold or obtain any Commission license or authorization.

5. Accordingly, **IT IS ORDERED** that, pursuant to Section 4(i) of the Act³ and the authority delegated by Sections 0.111 and 0.311 of the Rules⁴ the attached Consent Decree **IS ADOPTED** and its terms incorporated by reference.

6. **IT IS FURTHER ORDERED** that the above-captioned matter **IS TERMINATED**.

7. **IT IS FURTHER ORDERED** that a copy of this Order and Consent Decree shall be sent by first class mail and certified mail, return receipt requested, to Mr. James Talbot and Ms. Jackie Flemming, AT&T Services, 1120 20th St. NW, Suite 1000, Washington, DC 20036.

FEDERAL COMMUNICATIONS COMMISSION

Travis LeBlanc
Chief
Enforcement Bureau

***2810 CONSENT DECREE**

1. The Enforcement Bureau of the Federal Communications Commission and AT&T Services, Inc. (AT&T or Company), by their authorized representatives, hereby enter into this Consent Decree for the purpose of terminating the Enforcement Bureau's investigation into whether AT&T violated Sections 201(b) and 222¹ of the Communications Act of 1934, as amended (Communications Act or Act),² and Sections 64.2010(a) and 64.2011(b) of the Commission's Rules³ in connection with a data breach.

I. DEFINITIONS

2. For the purposes of this Consent Decree, the following definitions shall apply:

(a) "Act" means the Communications Act of 1934, as amended.

(b) "Adopting Order" means an order of the Bureau adopting the terms of this Consent Decree without change, addition, deletion, or modification.

(c) "Affected Customer" means any AT&T customer whose account was accessed without the customer's authorization by an employee of a call center in Colombia or the Philippines for the purpose of obtaining unlock codes.

****3** (d) "AT&T" or "Company" means AT&T Services, Inc., and its affiliates, subsidiaries, predecessors-in-interest, and successors-in-interest.

(e) "Bureau" means the Enforcement Bureau of the Federal Communications Commission.

(f) "Commission" and "FCC" mean the Federal Communications Commission and all of its bureaus and offices.

(g) "Call Center" means call centers operated by AT&T Mobility or its contractor(s) that provide mobility customer service or wireless sales service for AT&T Mobility consumer customers.

(h) “Communications Laws” means, collectively, the Act, the Rules, and the published and promulgated orders and decisions of the Commission to which AT&T is subject by virtue of its business activities.

***2811** (i) “Compliance Plan” means the compliance obligations, program, and procedures described in this Consent Decree at paragraph 18.

(j) “Covered Employees” means all employees and agents of AT&T who perform or directly supervise, oversee, or manage the performance of duties that involve access to, use, or disclosure of Personal Information or Customer Proprietary Network Information at Call Centers managed and operated by AT&T Mobility. Covered Employees do not include Covered Vendor Employees.

(k) “Covered Vendor Employees” means all employees and agents of Vendors who perform or directly supervise, oversee, or manage the performance of duties that involve access to, use, or disclosure of Personal Information or CPNI at Vendor Call Centers that provide customer service and wireless sales services for AT&T Mobility customers.

(l) “Customer Proprietary Network Information” and “CPNI” shall have the meaning set forth at Section 222(h)(1) of the Act.

(m) “CPNI Rules” means the rules set forth at 47 C.F.R. § 64.2001 *et seq.* and any amendments or additions to those rules subsequent to the Effective Date.

(n) “Data Breach” means access to a customer's account without authorization for the purpose of obtaining the customer's name, cellular telephone number, and last four digits of the customer's Social Security number to be used to obtain an unlock code.

(o) “Effective Date” means the date by which both the Bureau and AT&T have signed the Consent Decree.

(p) “Investigation” means the investigation commenced by the Bureau in EB-TCD-14-00016243.

(q) “Operating Procedures” means the standard internal operating procedures and compliance policies established by AT&T to implement the Compliance Plan.

(r) “Parties” means AT&T and the Bureau, each of which is a “Party.”

(s) “Personal Information” means either of the following: (1) an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social Security number; (B) driver's license number or other government-issued identification card number; or (C) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (2) a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

****4** (t) “Rules” means the Commission's regulations, found in Title 47 of the Code of Federal Regulations.

(u) “Vendor” means a third-party that operates and/or manages a Call Center on behalf of AT&T Mobility and provides customer service and wireless sales services for AT&T Mobility consumer customers.

***2812 II. BACKGROUND**

3. Section 222(c) of the Act, entitled “Confidentiality of Customer Proprietary Network Information,” restricts carriers’ use and disclosure of CPNI.⁴ Section 222(c)(1) only permits a carrier to disclose, permit access to, or use a customer’s individually identifiable CPNI to provide telecommunications services, or other services “necessary to, or used in,” the carrier’s telecommunications service, unless otherwise authorized by the customer or required by law.⁵

4. The Commission has adopted rules implementing Section 222(c)’s protections of CPNI. Section 64.2010(a) of the Commission’s Rules requires that “carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI.”⁶ Section 64.2011(b) requires a telecommunications carrier to notify designated law enforcement authorities of a “breach” of its customers’ CPNI “[a]s soon as practicable, in no event later than seven (7) business days, after reasonable determination of the breach”⁷ A “breach” occurs “when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.”⁸ A telecommunications carrier must provide notice of a breach to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through an online portal.⁹

5. Section 201(b) of the Act states, in part, that “[a]ll charges, practices, classifications, and regulations for and in connection with [interstate or foreign] communication service [by wire or radio], shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful.”¹⁰ The Notice of Apparent Liability in *TerraCom* states that Section 201(b) applies to carriers’ practices for protecting customers’ PII and CPNI.¹¹

6. AT&T is a telecommunications carrier that provides mobile voice and data services to customers throughout the United States, with its principal place of business in Dallas, Texas.¹² AT&T is the second largest wireless carrier in the United States, with over 100 million subscribers, earning \$126.4 billion in revenue in 2012 and \$128.8 billion in 2013.¹³

7. In May 2014, the Enforcement Bureau (Bureau) began investigating an internal Data Breach that occurred between November 2013 and April 2014 at a facility in Mexico under contract with *2813 AT&T (the April 2014 Breach). The Bureau’s investigation¹⁴ into the April 2014 Breach was based on reports submitted by AT&T to the Commission’s CPNI Data Breach Portal¹⁵ and publicly available information.¹⁶ AT&T informed the Bureau that it discovered that three employees of an AT&T Vendor that provided Spanish-language customer support services from an inbound Call Center located in Mexico (Mexico Call Center), had used login credentials to access customer accounts to obtain customer information—specifically, names and the last four digits of customers’ Social Security numbers—that could then be used to submit online requests for cellular handset unlock codes.¹⁷

****5** 8. AT&T maintained and operated the systems the Mexico Call Center employees used to access AT&T customer records. These systems were governed by AT&T’s data security measures.¹⁸ In this case, those measures failed to prevent or timely detect a large and ongoing Data Breach. The April 2014 Breach lasted 168 days (from November 4, 2013, until April 21, 2014). During this period, the three Mexico Call Center employees accessed 68,701 customers’ accounts, without authorization to obtain the above-referenced information required for unlock codes, which appeared on the same account page as these customers’ CPNI.¹⁹ Beginning in December 2013, more than 11,000 customer accounts were accessed each month until March 2014.²⁰ AT&T also determined that the personal information of 51,422 of these customers was used to place 290,803 handset unlock requests through AT&T’s online customer unlock request portal.²¹ Although CPNI appeared on the same page as the information required for unlock codes, AT&T found no evidence that the Mexico Call Center employees used or disclosed CPNI in connection with the data breach. In December 2012,

an AT&T employee became suspicious that an employee at the Mexico Call Center was possibly providing customer information to unauthorized persons.²² The Mexico Call Center employee was terminated by the Mexico Call Center for accessing customer accounts without leaving account notations.²³ In January 2013, AT&T discovered information *2814 that another at the Mexico Call Center may have engaged in suspicious activities suggesting access to accounts for an improper purpose.²⁴ This employee left the Mexico Call Center voluntarily prior to the completion of AT&T's investigation.²⁵ AT&T did not classify the 2012 and 2013 incidents as CPNI breaches at the time that they occurred because AT&T did not conclude that the breaches included use or disclosure of CPNI. Following the April 2014 Breach, however, AT&T re-examined these incidents and reported them to the USSS and FBI via the CPNI breach reporting portal in September 2014.²⁶

9. AT&T commenced its investigation of the April 2014 Breach on April 3, 2014, and notified members of its senior management of the investigation on April 4, 2014.²⁷ According to AT&T, "it was quickly apparent that the incident potentially involved a high volume of customer account access."²⁸ AT&T was aware from the outset of its investigation that the customer database that was accessed to perpetrate the suspected breach contained billing information and other CPNI.²⁹ On April 8, 2014, the Mexico Call Center, in consultation with AT&T, interviewed one of the employees suspected of engaging in the breach, concluded that the employee presented an "evasive attitude" during the interview, and, after conducting a polygraph examination of the employee, severed him from his job functions and began the process to terminate his employment.³⁰ By April 22, 2014, AT&T had received the imaged hard drives from computers believed to have been involved in the breach, and began its forensic analysis shortly thereafter.³¹ On May 20, 2014, AT&T notified the USSS and the FBI of the incident.³² As noted above, Section 64.2011(b) requires a carrier to notify law enforcement of a CPNI breach "[a]s soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach"³³ AT&T reported completing notification to customers affected by the breach on July 3, 2014.³⁴

*6 10. AT&T informed the Bureau that it terminated its use of the Mexico Call Center on September 28, 2014.³⁵

11. In March 2015, AT&T disclosed to the Bureau that it was investigating additional potential Data Breaches in Colombia and the Philippines. AT&T informed the Bureau that its *2815 investigation was ongoing but that thus far it had discovered that call center employees in Bogota, Colombia and the Philippines had accessed customer accounts in order to obtain unlock codes for AT&T mobile phones. In Bogota, until May 27, 2014, full Social Security numbers were accessible in the ordinary course of business to three of the managers whose login credentials were used in these activities. After May 27, 2014, AT&T implemented measures to mask full Social Security numbers for AT&T Mobility Call Center managers. AT&T has found no evidence that these or any other managers in Colombia or the Philippines acquired or used the full Social Security numbers of any Affected Customers. In some cases, certain CPNI relating to bill amounts and rate plans were visible at the time of the unauthorized activity, but AT&T's investigation also found no evidence that this information was used. The unauthorized access ceased in the Bogota, Colombia facility in July 2014. In December 2014, AT&T changed its unlock policy and ceased requiring information from customer records before providing an unlock code. This change eliminated the incentive for Covered Employees or Covered Vendor Employees to engage in the activities described above. AT&T informed the Bureau that based on its investigation to date, it had identified approximately 211,000 customer accounts that were accessed in connection with the unlock code activities in the Colombian and Philippines facilities, but that its ongoing investigation could reveal additional instances of such activities. AT&T informed the Bureau that it is in the process of developing new monitoring procedures to identify suspicious account access by call center representatives.

12. The Parties negotiated the following terms and conditions of settlement and hereby enter into this Consent Decree as provided below.

III. TERMS OF AGREEMENT

13. **Adopting Order.** The provisions of this Consent Decree shall be incorporated by the Bureau in an Adopting Order.

14. **Jurisdiction.** AT&T agrees that the Bureau has jurisdiction over it and the matters contained in this Consent Decree and has the authority to enter into and adopt this Consent Decree.

15. **Effective Date; Violations.** The Parties agree that this Consent Decree shall become effective on the Effective Date as defined herein. As of the Effective Date, the Parties agree that this Consent Decree shall have the same force and effect as any other order of the Commission.

16. **Termination of Investigation.** In express reliance on the covenants and representations in this Consent Decree and to avoid further expenditure of public resources, the Bureau agrees to terminate the Investigation and its investigation into matters described in paragraph 11. In consideration for the termination of the Investigation, AT&T agrees to the terms, conditions, and procedures contained herein. The Bureau further agrees that, in the absence of new material evidence relating to the Investigation, it will not use the facts developed in the Investigation through the Effective Date, or the existence of this Consent Decree, to institute any new proceeding, formal or informal, or take any action against AT&T concerning the matters that were the subject of the Investigation, including the matters described in paragraphs 7 through 10, and its investigation into matters described in paragraph 11. The Bureau also agrees that, in the absence of new material evidence relating to the Investigation described in paragraphs 7-10, the investigation into matters described in paragraph 11 and in the absence of any misrepresentation in paragraph 19(a), it will not use the facts developed in the Investigation or its investigation into matters described in paragraph 11 through the Effective Date, or the existence of this Consent Decree, to institute any proceeding, formal or informal, or take any action against AT&T with respect to basic qualifications, including its character qualifications, to be a Commission licensee or hold Commission licenses or authorizations. For purposes of this paragraph, additional instances of unauthorized access to a customer's account in Colombia or the Philippines for the apparent purpose of obtaining an unlock code do not constitute new material evidence. For the purpose of this Consent Decree only, AT&T does not contest that its actions that were the subject of the Investigation violated Section 222(c) of the Act, and Sections 64.2010(a) and 64.2011(b) of the Commission's Rules. It is the intent of the Parties that this Consent Decree shall not be used as evidence or precedent in any action or proceeding, except in an action to enforce the Consent Decree.

****7 17. Compliance Officer.** Within thirty (30) calendar days after the Effective Date, AT&T shall designate a senior corporate manager with the requisite corporate and organizational authority to serve as a Compliance Officer and to discharge the duties set forth below. The person designated as the Compliance Officer shall be responsible for developing, implementing, and administering the Compliance Plan and ensuring that AT&T complies with the terms and conditions of the Compliance Plan and this Consent Decree. In addition to the general knowledge of the Communications Laws necessary to discharge his or her duties under this Consent Decree, the Compliance Officer shall have specific knowledge of the information security principles and practices necessary to implement the information security requirements of this Consent Decree, and the specific requirements of Section 222 of the Act, and the CPNI Rules, before assuming his/her duties. The Compliance Officer or managers reporting to the Compliance Officer with responsibilities related to this Consent Decree shall be privacy certified by an industry certifying organization and keep current through appropriate continuing privacy education courses.

18. **Compliance Plan.** For purposes of settling the matters set forth herein, AT&T agrees that it shall, within ninety (90) calendar days after the Effective Date, develop and implement a Compliance Plan designed to ensure future compliance with the Communications Laws and with the terms and conditions of this Consent Decree. AT&T will implement, at a minimum, the following procedures:

(a) **Risk Assessment.** Within ninety (90) calendar days after the Effective Date, AT&T shall complete a risk assessment reasonably designed to identify internal risks of unauthorized access, use, or disclosure of Personal Information and

CPNI by Covered Employees and Covered Vendor Employees (Risk Assessment). The Risk Assessment must evaluate the sufficiency of existing policies, procedures, and other safeguards in place to control the risk of such unauthorized access, use, or disclosures.

(b) **Information Security Program.** Within ninety (90) calendar days after the Effective Date, AT&T shall have in place and thereafter maintain an information security program reasonably designed to protect CPNI and Personal Information from unauthorized access, use, or disclosure by Covered Employees and Covered Vendor Employees (Information Security Program). AT&T shall ensure that the Information Security Program is fully documented in writing (including, as appropriate, within the Operating Procedures/Compliance Manual described below) and includes: (i) administrative, technical, and physical safeguards reasonably designed to protect the security and confidentiality of Personal Information and CPNI; (ii) reasonable measures to protect Personal Information and CPNI maintained by or made available to Vendors, Covered Employees, and Covered Vendor Employees, including exercising due diligence in selecting Vendors, requiring Vendors by contract to implement and maintain administrative, technical, and physical safeguards for the protection of Personal Information and CPNI, and engaging in ongoing monitoring of Vendors' compliance with their security obligations and implementing measures to sanction Vendors that fail to comply with their security obligations (including, where appropriate, terminating AT&T's relationship with such Vendors); (iii) access controls reasonably designed to limit access to Personal Information and CPNI to authorized AT&T employees, agents, and Covered Vendor Employees; (iv) reasonable processes to assist AT&T in detecting and responding to suspicious or anomalous account activity, including whether by malware or otherwise, involving Covered Employees and Covered Vendor Employees; (v) a comprehensive breach response plan that will enable AT&T to fulfill its obligations under applicable laws, with regard to breach *2817 notifications, including its obligations under paragraph 20 while that paragraph remains in effect.

8 (c) **Ongoing Monitoring and Improvement. AT&T shall monitor its Information Security Program on an ongoing basis to ensure that it is operating in a manner reasonably calculated to control the risks identified through the Risk Assessment, to identify and respond to emerging risks or threats, and to comply with the requirements of Section 222 of the Act, the CPNI Rules, and this Consent Decree. To the extent that such monitoring reveals that the program is deficient or no longer reasonably fulfills this purpose, AT&T shall implement additional safeguards to address these deficiencies and gaps. Such additional safeguards shall be implemented within a reasonable period of time, taking into account the seriousness of the deficiencies or gaps and the steps necessary to address them.

(d) **Compliance Review.** Within ninety (90) calendar days after the Effective Date, AT&T shall commence a formal internal review of its Information Security Program using procedures and standards generally accepted in the information privacy field. This formal internal review shall be directed by AT&T's Corporate Compliance Unit by professionals with the requisite privacy certifications necessary to review and assess information security programs. Such assessment shall be completed within one hundred and fifty (150) calendar days after the Effective Date, and AT&T shall submit a copy of the written assessment findings to the Commission within ten (10) calendar days of the assessment's completion.

(e) **Compliance Manual.** Within one hundred and twenty (120) calendar days after the Effective Date, the Compliance Officer shall develop and distribute a Compliance Manual to all Covered Employees and to all Vendors with instructions to Vendors to distribute a copy of the Compliance Manual to all Covered Vendor Employees within thirty (30) days and to certify that such distribution has been completed. If such certification is not provided, AT&T will pursue any remedy available to require distribution and certification, including, if necessary, termination of the relationship. Additionally, AT&T shall instruct all Vendors to deliver a Compliance Manual to all future Covered Vendor Employees within thirty (30) calendar days after such future Covered Vendor Employee assumes such position or responsibilities.

(f) The Compliance Manual shall explain the requirements of Sections 222 of the Act, the CPNI Rules, and this Consent Decree, and set forth the Operating Procedures that Covered Employees and Covered Vendor Employees shall follow to help ensure AT&T's compliance with the Act, Rules, and this Consent Decree. AT&T shall periodically review and

revise the Compliance Manual and Operating Procedures as necessary to ensure that the information set forth therein remains current and accurate. AT&T shall distribute any revisions to the Compliance Manual to all Covered Employees and all Vendors within thirty (30) calendar days of making such revisions.

****9 (g) Compliance Training Program.** AT&T shall establish and implement a Compliance Training Program on compliance with [Section 222](#), the CPNI Rules, and the Operating Procedures. As part of the Compliance Training Program Covered Employees shall be advised of AT&T's reporting obligations under paragraph 20 of this Consent Decree and shall be instructed on how to disclose noncompliance with [Section 222](#), the CPNI Rules and the Operating Procedures to the Compliance Officer or his designees. All Covered Employees shall be trained pursuant to the Compliance Training program within six (6) months after the Effective Date, and, any person who becomes a Covered Employee at any time after the initial Compliance Training Program shall be trained within thirty (30) calendar days after the date such person becomes a Covered Employee. AT&T shall repeat compliance training on an annual basis, and shall periodically review and revise the Compliance Training Program as necessary to ensure that it remains current and complete and to enhance its effectiveness. AT&T shall request, and where permitted by contract require, all Vendors to provide the training to all Covered Vendor Employees within six (6) months after the Effective Date, except that any person who becomes a Covered Vendor Employee at any time after the initial Compliance Training Program shall be trained within thirty (30) calendar days after the date such person becomes a Covered Vendor Employee. AT&T shall request, and where permitted by contract, require Vendors to repeat compliance training on an annual basis.

19. Terms Specific to Call Centers in Colombia and the Philippines.

(a) AT&T represents and warrants that it engaged independent third parties to investigate the activities in Bogota, Colombia and to assist with employee interviews in connection with AT&T's investigation of call centers in the Philippines. AT&T further represents and warrants that it has no evidence and no reason to believe that any CPNI or any Personal Information was obtained or used during the course of the activities described in paragraphs 7-11, AT&T further represents and warrants that, effective December 11, 2014, it changed its device unlock policy and no longer requires information contained in AT&T customer records in order to obtain an unlock code, thereby eliminating the incentive for the activities described in paragraphs 7-11. After reasonable diligence, and based on information currently available, including AT&T's change in its unlock policy, AT&T believes that the activities described in paragraph 11 have ceased. AT&T further represents and warrants that it has reported to the Bureau all known instances in which it has reasonably concluded that a Data Breach occurred in Colombia and Philippines call centers. AT&T further represents and warrants that it is continuing to investigate call centers in Colombia and the Philippines for Data Breaches.

****10 (b)** Within thirty (30) calendar days of the Effective Date, AT&T shall:

- i. Begin a process to provide each Affected Customer written notice that his or her account, including Personal Information and/or CPNI, had been accessed by persons without authorization in violation of AT&T's privacy and security policies and include an offer of one year of complimentary credit monitoring services through a nationally recognized credit monitoring service, such as CSID Protector. The complimentary credit monitoring services offered to each Affected Customer shall include, at a minimum, single bureau credit report and monitoring; court record monitoring and public records searches; non-credit loan searches; identity theft insurance at no cost to Affected Customers; and full service identity theft restoration services. Each written notice provided to Affected Customers shall include the toll-free telephone numbers and web addresses of the major credit reporting agencies. AT&T shall complete such notification within 60 days.
- ii. AT&T shall provide a toll-free number where Affected Customers may contact AT&T with questions about the impact of these activities, if any, on their account information.

*2819 iii. Subparagraphs 19(b)(i)-(ii) shall also apply to Affected Customers who are identified after the Effective Date and AT&T shall provide the notice required pursuant to subparagraph 19(b) to such customers within thirty (30) calendar days of AT&T's discovery that such customers' accounts were illegally accessed.

20. **Reporting Noncompliance and Data Breaches.** AT&T shall report any noncompliance with the terms and conditions of this Consent Decree within fifteen (15) calendar days after discovery of such noncompliance. Such reports shall include a detailed explanation of: (i) each known instance of noncompliance; (ii) the steps that AT&T has taken or will take to remedy such noncompliance; (iii) the schedule on which such remedial actions will be taken; and (iv) steps that AT&T has taken or will take to prevent the recurrence of any such noncompliance. AT&T shall also report to the FCC any breaches of Personal Information or CPNI involving any Covered Employees or Covered Vendor Employees that AT&T is required by any federal or state law to report to any Federal or state entity or any individual. Reports shall be submitted no later than seven (7) business days after completion of the notification required by federal or state authorities. Such reports shall include (i) the date the breach was reported, (ii) the applicable Federal and state authorities to whom the breach was reported, (iii) copies of the reports AT&T submitted to the applicable state authorities, and (iv) the reference number generated by the central reporting facility for CPNI reports made pursuant to 47 C.F.R. § 64.2011(b). All reports of noncompliance shall be submitted to the Chief, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, 445 12th Street, SW, Rm. 4C-224, Washington, DC 20554, with copies submitted electronically to David.Valdez@fcc.gov and Michael.Epshteyn@fcc.gov. The foregoing reporting requirement does not affect AT&T's obligations to report data breaches to other regulatory authorities in accordance with applicable law.

11 21. **Compliance Reports. AT&T shall file compliance reports with the Commission six (6) months after the Effective Date, twelve (12) months after the Effective Date, twenty-four (24) months after the Effective Date, and thirty-six (36) months after the Effective Date.

(a) Each Compliance Report shall include a detailed description of AT&T's efforts during the relevant period to comply with the terms and conditions of this Consent Decree. In addition, each Compliance Report shall include a certification by the Compliance Officer, as an agent of and on behalf of AT&T, stating that the Compliance Officer has personal knowledge that AT&T: (i) has established and implemented the Compliance Plan; (ii) has utilized the Operating Procedures since the implementation of the Compliance Plan; and (iii) is not aware of any instances of noncompliance with the terms and conditions of this Consent Decree, including the reporting obligations set forth in paragraph 20 of this Consent Decree.

(b) The Compliance Officer's certification shall be accompanied by a statement explaining the basis for such certification and shall comply with Section 1.16 of the Rules and be subscribed to as true under penalty of perjury in substantially the form set forth therein.³⁶

(c) If the Compliance Officer cannot provide the requisite certification, the Compliance Officer, as an agent of and on behalf of AT&T, shall provide the Commission with a detailed explanation of the reason(s) why and describe fully: (i) each instance of noncompliance; (ii) the steps that AT&T has taken or will take to remedy such noncompliance, including the schedule on which proposed remedial actions will be taken; and (iii) the steps that AT&T has taken or will take to prevent the recurrence of any such noncompliance, including the schedule on which such preventive action will be taken.

*2820 (d) All Compliance Reports shall be submitted to the Chief, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, 445 12th Street, SW, Rm. 4C-224, Washington, DC 20554, with a copy submitted electronically to David.Valdez@fcc.gov and Michael.Epshteyn@fcc.gov.

22. **Termination Date.** With the exception of paragraphs 18(b)-(c), the requirements set forth in paragraphs 17 through 21 of this Consent Decree shall expire thirty-six (36) months after the Effective Date. The requirements set forth in paragraphs 18(b)-(c) shall expire seven (7) years after the Effective Date.

23. **Section 208 Complaints; Subsequent Investigations.** Nothing in this Consent Decree shall prevent the Commission or its delegated authority from adjudicating complaints filed pursuant to Section 208 of the Act³⁷ against AT&T or its affiliates for alleged violations of the Act, or for any other type of alleged misconduct, regardless of when such misconduct took place. The Commission's adjudication of any such complaint will be based solely on the record developed in that proceeding. Except as expressly provided in this Consent Decree, this Consent Decree shall not prevent the Commission from investigating new evidence of noncompliance by AT&T with the Communications Laws.

****12 24. Civil Penalty.** AT&T will pay a civil penalty to the United States Treasury in the amount of \$ 25 million (\$25,000,000) within thirty (30) calendar days after the Effective Date. AT&T shall send electronic notification of payment to Johnny Drake, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission at Johnny.Drake@fcc.gov on the date said payment is made. The payment must be made by check or similar instrument, wire transfer, or credit card, and must include the Account Number and FRN referenced above. Regardless of the form of payment, a completed FCC Form 159 (Remittance Advice) must be submitted.³⁸ When completing the FCC Form 159, enter the Account Number in block number 23A (call sign/other ID) and enter the letters "FORF" in block number 24A (payment type code). Below are additional instructions that should be followed based on the form of payment selected:

- Payment by check or money order must be made payable to the order of the Federal Communications Commission. Such payments (along with the completed Form 159) must be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank — Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.

- Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. To complete the wire transfer and ensure appropriate crediting of the wired funds, a completed Form 159 must be faxed to U.S. Bank at (314) 418-4232 on the same business day the wire transfer is initiated.

- Payment by credit card must be made by providing the required credit card information on FCC Form 159 and signing and dating the Form 159 to authorize the credit card payment. The completed Form 159 must then be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank — Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.

Questions regarding payment procedures should be addressed to the Financial Operations Group Help Desk by phone, 1-877-480-3201, or by e-mail, ARINQUIRIES @fcc.gov.

***2821 25. Waivers.** As of the Effective Date, AT&T waives any and all rights it may have to seek administrative or judicial reconsideration, review, appeal or stay, or to otherwise challenge or contest the validity of this Consent Decree and the Adopting Order. AT&T shall retain the right to challenge Commission interpretation of the Consent Decree or any terms contained herein. If either Party (or the United States on behalf of the Commission) brings a judicial action to enforce the terms of the Consent Decree or the Adopting Order, neither AT&T nor the Commission shall contest the validity of the Consent Decree or the Adopting Order, and AT&T shall waive any statutory right to a trial *de novo*. AT&T hereby agrees to waive any claims it may otherwise have under the Equal Access to Justice Act³⁹ relating to the matters addressed in this Consent Decree.

****13 26. Severability.** The Parties agree that if any of the provisions of the Consent Decree shall be held unenforceable by any court of competent jurisdiction, such unenforceability shall not render unenforceable the entire Consent Decree, but rather the entire Consent Decree shall be construed as if not containing the particular unenforceable provision or provisions, and the rights and obligations of the Parties shall be construed and enforced accordingly.

27. Invalidity. In the event that this Consent Decree in its entirety is rendered invalid by any court of competent jurisdiction, it shall become null and void and may not be used in any manner in any legal proceeding.

28. Subsequent Rule or Order. The Parties agree that if any provision of the Consent Decree conflicts with any subsequent Rule or Order adopted by the Commission (except an Order specifically intended to revise the terms of this Consent Decree to which AT&T does not expressly consent) that provision will be superseded by such Rule or Order.

29. Successors and Assigns. AT&T agrees that the provisions of this Consent Decree shall be binding on its successors, assigns, and transferees.

30. Final Settlement. The Parties agree and acknowledge that this Consent Decree shall constitute a final settlement between the Parties with respect to the Investigation.

31. Modifications. Except as provided in paragraph 27, this Consent Decree cannot be modified without the advance written consent of both Parties.

32. Paragraph Headings. The headings of the paragraphs in this Consent Decree are inserted for convenience only and are not intended to affect the meaning or interpretation of this Consent Decree.

33. Authorized Representative. Each Party represents and warrants to the other that it has full power and authority to enter into this Consent Decree. Each person signing this Consent Decree on behalf of a Party hereby represents that he or she is fully authorized by the Party to execute this Consent Decree and to bind the Party to its terms and conditions.

***2822 34. Counterparts.** This Consent Decree may be signed in counterpart (including electronically or by facsimile). Each counterpart, when executed and delivered, shall be an original, and all of the counterparts together shall constitute one and the same fully executed instrument.

—
Travis LeBlanc, Chief

Enforcement Bureau

—
Date

For: AT&T Services, Inc.

—
Debbie Storey

Executive Vice President — Mobility Customer Service

AT&T Services, Inc.

—
Date

Footnotes

- 1 *See* 47 U.S.C. §§ 201, 222.
- 2 *See* 47 C.F.R. §§ 64.2010(a), 64.2011(b).
- 3 47 U.S.C. § 154(i).
- 4 47 C.F.R §§ 0.111, 0.311.
- 1 47 U.S.C. §§ 201(b), 222.
- 2 47 U.S.C. § 151 *et seq.*
- 3 47 C.F.R. §§ 64.2010(a), 64.2011(b).
- 4 *See* 47 U.S.C. § 222(c).
- 5 *Id.* at § 222(c)(1).
- 6 47 C.F.R. § 64.2010(a).
- 7 47 C.F.R. § 64.2011(b).
- 8 47 C.F.R. § 64.2011(e).
- 9 47 C.F.R. § 64.2011(b). The Commission maintains a link to the portal at <http://www.fcc.gov/eb/cpni>. Telecommunications carriers are required to report CPNI data breaches via the online portal accessible through that site. The data reported through the FCC portal is collected by U.S. Secret Service and the Federal Bureau of Investigation.
- 10 47 U.S.C. § 201(b).
- 11 *TerraCom, Inc. and YourTel America, Inc., Notice of Apparent Liability for Forfeiture*, 29 FCC Rcd 13325, 13335-36, paras. 31-32 (2014).
- 12 AT&T is an interexchange carrier (499 Filer ID Number: 806172). New Cingular Wireless Services, Inc. CONSOLIDATED, is listed as providing Cellular/PCS/SMR services and doing business as AT&T Mobility (499 Filer ID Number: 821002). AT&T's principal place of business is located at 208 S. Akard Street, Dallas, TX 75202. Randall Stephenson is the Chief Executive Officer.
- 13 *See AT&T's 2013 Annual Report*, http://www.att.com/Investor/ATT_Annual/2013/financial_highlights.html (lasted visited Jan. 20, 2015).
- 14 The Bureau issued two Letters of Inquiry (LOIs) to AT&T, seeking information about the April 2014 Breach, other reported security breaches, and AT&T's data security practices generally. *See* Letter from Richard A. Hindman, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Jackie Flemming, AT&T Services, Inc. (June 30, 2014) (on file in EB-TCD-14-00016243); *see also* Letter from Richard A. Hindman, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Jackie Flemming, AT&T Services, Inc. (November 7, 2014) (on file in EB-TCD-14-00016243). AT&T responded to the LOI on July 29, 2014. *See* Letter from James Talbot, General Attorney, AT&T, to Richard A. Hindman, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (July 29, 2014) (on file in EB-TCD-14-00016243) (LOI Response). AT&T submitted a response to the Supplemental LOI on December 8, 2014. *See* Letter from James Talbot, General Attorney, AT&T, to Richard A. Hindman, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Dec. 8, 2014) (on file in EB-TCD-14-00016243) (Supplemental LOI Response).
- 15 *See supra* note 9.
- 16 AT&T reported the April 2014 Breach to the California Attorney General. *See* Submitted Breach Notification Sample, State of California Department of Justice, Office of the Attorney General, <http://oag.ca.gov/ecrime/databreach/reports/sb24-45415> (lasted visited Dec. 19, 2014); *see also* Martyn Williams, *AT&T says customer data accessed to unlock smartphones*, ITWORLD (June 12, 2014), <http://www.itworld.com/article/2695622/security/at-t-says-customer-data-accessed-to-unlock-smartphones.html> (last visited Jan. 29, 2015).
- 17 *See* LOI Response at 19.
- 18 *See* Supplemental LOI Response at 6.

- 19 See LOI Response at 5-6, 20.
20 See LOI Response at 5.
21 See LOI Response at 21.
22 See Supplemental LOI Response at 8-9.
23 See Supplemental LOI at 9.
24 *Id.*
25 *Id.*
26 See Supplemental LOI Response at 8-9. In December 2014, AT&T identified additional customer accounts that appeared to have been accessed by these employees in 2012. AT&T treated these incidents as CPNI breaches and reported them via the online portal. See Supplemental LOI Response at 9-10.
27 See LOI Response at 6.
28 LOI Response at 15.
29 See LOI Response at 1.
30 See LOI Response at 17.
31 See LOI Response at 17.
32 See LOI Response at 20.
33 47 C.F.R. § 64.2011(b).
34 See LOI Response at 7. AT&T determined that approximately 156 prepaid customers, however, did not have valid physical addresses or email addresses and those customers were notified via SMS message on July 10, 2014.
35 See Letter from James Talbot, General Attorney, AT&T, to Richard A. Hindman, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Jan. 23, 2015) (on file in EB-TCD-14-00016243); see also e-mail from James Talbot, Attorney, AT&T Services, Inc., to Rosemary Cabral, Attorney-Advisor, Telecommunications Consumers Division, FCC Enforcement Bureau (Jan. 27, 2015, 15:42 EDT).
36 See 47 C.F.R. § 1.16.
37 47 U.S.C. § 208.
38 An FCC Form 159 and detailed instructions for completing the form may be obtained at <http://www.fcc.gov/Forms/Form159/159.pdf>.
39 See 5 U.S.C. § 504; 47 C.F.R. §§ 1.1501-1.1530.
30 FCC Rcd. 2808 (F.C.C.), 30 F.C.C.R. 2808, 62 Communications Reg. (P&F) 526, 2015 WL 1577197

End of Document

© 2018 Thomson Reuters. No claim to original U.S. Government Works.

EXHIBIT “B”

About Our Privacy Policy

Whenever you do something like buy one of our products, watch a show or download an app, information is created. Because we know your privacy is important, we have a Privacy Policy to explain how we collect, use and protect that information. There's a quick summary below, and the actual policy is written in **an easy to understand "Frequently Asked Questions" (FAQ) format (/sites/privacy_policy/terms)**. We want to simplify this explanation, so you can make informed choices about your privacy, and then spend the rest of your time enjoying our products and services.

Effective May 2, 2017

A Quick Summary of Our Privacy Policy

Our Privacy Policy applies to your use of all products, services and websites offered by AT&T and our AT&T affiliates, such as DIRECTV, unless they have a different privacy policy. Because some apps, including some AT&T and DTV branded apps, require additional information, or use information in different ways, they may have their own privacy policies and/or terms and conditions. These apps may also offer you additional choices for managing your personal information.

Back to Top

Our privacy commitments

- We don't sell your Personal Information to anyone for any purpose. Period.
- We keep your Personal Information in our business records while you are a customer, or until it is no longer needed for business, tax or legal purposes.
- We will keep your information safe using encryption or other appropriate security controls.

Back to Top

Here's some of the information we collect:

- **Account Information** includes your name, address, telephone number, e-mail address, service-related details such as payment data, security codes, service history and other information like that;
- **Network Performance & Usage Information** tells us how you use our networks, our products and our services, and how well our equipment and networks are performing;
- **Web Browsing & Wireless Application Information** tells us about the websites you visit and the mobile applications you use on our networks;
- **Location Information** tells us where your wireless device is located, as well as your ZIP-code and street address;
- **TV Viewing Information** tells us about which programs you watch and record and similar information about how you use our video services and applications.

Back to Top

Here are the three basic ways we collect it:

- We get information from you when you do things like make a purchase from us;
- We collect it from how you use our products and services;
- We obtain information from other sources, like credit agencies, marketing companies, and other service providers.

Back to Top

Here are just some of the ways we use it. To:

- Provide services and improve your customer experience;
- Send you bills for your services;
- Respond to your questions;
- Address network integrity, help in fraud prevention and network and device security issues;
- Do research and analysis to maintain, protect, develop and improve our networks and services;

- Let you know about service updates, content, offers and promotions that may be of interest to you;
- Improve entertainment options;
- Deliver Relevant Advertising;
- Create External Marketing & Analytics Reports;
- Assist in the prevention and investigation of illegal activities and violations of our Terms of Service or Acceptable Use Policies.

Back to Top

Some examples of who we share your Personal Information with:

- **Across our companies** to give you the best customer experience and to help you get everything we have to offer.
- **Other, non-AT&T companies that perform services on our behalf** only as needed for them to perform those services. We require them to protect your information consistent with our Policy.
- **With other companies and entities, to:**
 - Respond to 911 requests and other emergencies or exigencies;
 - Comply with court orders and other legal process;
 - Assist with identity verification, and preventing fraud and identity theft;
 - Enforce our agreements and property rights;
 - and Obtain payment for products and services including the transfer or sale of delinquent accounts to third parties for collection

Back to Top

Understanding Personal, Anonymous & Aggregate Information

- What is Personal Information? Information that identifies or reasonably can be used to identify you.
- What is Anonymous Information? This is information that doesn't identify you and can't reasonably be used to identify you specifically.
- What is Aggregate Information? We take a whole bunch of people's data and combine it into anonymous groups or categories.
- How do we use this information? We use and share this information in many ways including research, analysis, retail marketing, and Relevant Advertising. This data is also included in External Marketing & Analytics Reports.
- Want to learn more? Go [here \(/sites/privacy_policy/terms#aggregate\)](/sites/privacy_policy/terms#aggregate).

Back to Top

Our Online Privacy Policy for Children

- We want you to know that we don't knowingly collect personally identifying information from anyone under the age of 13 unless we first obtain permission from the child's parent or legal guardian.

Back to Top

Your Choices & Controls

- For information about children's safety and parental controls, view our **AT&T Smart Controls and DIRECTV Parental Controls (<https://www.att.com/shop/wireless/smartcontrols.html>)**.
- You have choices about certain types of advertising you get from us;
- You can control whether your anonymous information is used in our External Marketing & Analytics Reports;
- You can choose whether to receive marketing calls, e-mails or text messages or certain other communications from us;
- You have a choice about how we use your Customer Proprietary Network Information.

Back to Top.

Visit our **Privacy Policy (/sites/privacy_policy/full_privacy_policy)** for more information.

- **Definitions (/sites/privacy_policy/terms#definitions)**
- **Scope of this Policy (/sites/privacy_policy/terms#scope)**
- **The Information We Collect, How We Collect It, And How We Use It (/sites/privacy_policy/terms#collect)**
- **Information Sharing (/sites/privacy_policy/terms#sharing)**
- **Online Activity Tracking and Advertising (/sites/privacy_policy/terms#tracking)**
- **Location Information (/sites/privacy_policy/terms#location)**
- **Aggregate and Anonymous Information (/sites/privacy_policy/terms#aggregate)**
- **External Marketing & Analytics Reports (/sites/privacy_policy/terms#analytics)**

- [Online Privacy Policy for Children \(/sites/privacy_policy/terms#children\)](/sites/privacy_policy/terms#children)
- [Data Protection & Security \(/sites/privacy_policy/terms#protection\)](/sites/privacy_policy/terms#protection)
- [Changes \(/sites/privacy_policy/terms#changes\)](/sites/privacy_policy/terms#changes)
- [Choices & Controls \(/sites/privacy_policy/terms#controls\)](/sites/privacy_policy/terms#controls)
- [How to Contact Us \(/sites/privacy_policy/terms#contact\)](/sites/privacy_policy/terms#contact)

Your California Privacy Rights

California Civil Code Section 1798.83 entitles California customers to request information concerning whether a business has disclosed Personal Information to any third parties for their direct marketing purposes. As stated in this Privacy Policy, we will not sell your Personal Information to other companies and we will not share it with other companies for them to use for their own marketing purposes without your consent.

California Web Site Data Collection & "Do Not Track" Notices

Web Site Data Collection: We do not knowingly allow other parties to collect personally identifiable information about your online activities over time and across third-party web sites when you use our websites and services. We provide information about the opt-out choices available to customers, and the opt-out choices provided by certain third-party website and mobile application analytics companies we use [here \(/sites/privacy_policy/rights_choices\)](/sites/privacy_policy/rights_choices).

"Do Not Track" Notice: Because the providers of "do not track" and similar signals do not yet operate according to common, industry-accepted standards, we currently do not respond to those signals. For more information on Do Not Track, please visit www.allaboutdnt.com (<http://www.allaboutdnt.com/>).

California customers who wish to request further information about our compliance with these requirements, or have questions or concerns about our privacy practices and policies may contact us at privacypolicy@att.com (<mailto:privacypolicy@att.com>), or write to us at AT&T Privacy Policy, Chief Privacy Office, 208 S. Akard, Room 1033, Dallas, TX 75202.

Back to top

AT&T Privacy Policy FAQ

Our AT&T Privacy Policy in easy to understand, FAQ format.

We understand that everyone thinks that privacy policies are long, complicated and difficult to understand. So we're going to try to make this as simple as possible.

What is the purpose of AT&T's Privacy Policy? Whenever you do something like buy or use one of our products or services or visit our websites, information is created. Because we know privacy is important to you, we have the AT&T Privacy Policy to explain how we collect, use, protect, and share that created information. Thus, the main purpose of the Policy is to help you understand our relationship and how we are able to deliver and improve the services we offer.

How should this Policy be used? We encourage you to read the whole policy so you will understand fully our relationship. To find specific information, here is an outline of where you will find answers to your questions about key topics:

Visit these links for more information.

- [Definitions](#)
- [Scope of this Policy](#)
- [The Information We Collect, How We Collect It, And How We Use It](#)
- [Information Sharing](#)
- [Online Activity Tracking and Advertising](#)
- [Location Information](#)
- [Aggregate and Anonymous Information](#)
- [External Marketing & Analytics Reports](#)
- [Online Privacy Policy for Children](#)
- [Data Protection & Security](#)
- [Changes](#)
- [Choices & Controls](#)
- [How to Contact Us](#)

Definitions

Let's start with what we mean when we say:

Aggregate Information: We combine individual information into anonymous groups of customers or users. One way to think of it is in terms of a survey or opinion poll. Aggregate information would tell you that 80 percent of the people voted for a candidate, but not who actually voted. These groups are large enough to reasonably prevent individuals from being identified.

Anonymous Information: Information that doesn't directly identify and can't reasonably be used to identify an individual customer or user.

AT&T: Throughout this Policy, references to "AT&T," "we," "us," and "our" include the family of AT&T companies around the world except affiliates or applications with a separate privacy policy.

Customer: Anyone who purchases or uses our products or services. When a customer purchases retail products or services for use by others, like a family account, those family members also are customers.

Mobile Application: A software application that runs on smartphones, tablet computers or other mobile devices and that allows users to access a variety of services and information.

Personal Information: Information that directly identifies or reasonably can be used to figure out the identity of a customer or user, such as your name, address, phone number and e-mail address. Personal Information does not include published listing information.

Relevant Advertising: Creates aggregate audience segments based on non-personally identifiable information about customers (like age, ethnicity, income range, a particular geographic area, and their interests) to serve advertising that is more likely to be useful to those audience segments. "Online behavioral advertising" is one type of Relevant Advertising. It uses interest categories based on the websites visited by people who are not personally identified to deliver advertising online.

Third-Party Services: Services from third-party service providers other than AT&T, such as banks or roadside assistance companies.

User: Anyone who visits our websites or uses our mobile applications.

Website: And other terms like "Internet site," "site" and "web page" all mean the same thing, namely any page or location on the Internet, no matter what device (cell phone, tablet, laptop, PC, etc.) or protocol (http, WAP, ftp or other) is used to access the page or location.

Back to Top.

Questions about the Scope of this Policy

1. To whom does the Policy apply?

This Privacy Policy applies to customers and users of AT&T products and services, except customers and users of products or services provided by an affiliate or an application with a different privacy policy.

2. What does this Policy cover?

This Privacy Policy covers our practices regarding the information we collect about our customers and users (how we collect it and how we use it). Use of our products and services, as well as visits to our websites, are subject to this Privacy Policy.

3. Do you have any Privacy Policies other than this one?

Yes. Some AT&T affiliates or applications may have separate privacy policies that describe how they collect, use and share information they collect from their customers and users. When we share Personal Information with those affiliates or combine it with information from those applications we protect it in a way consistent with this Privacy Policy.

Additionally, some of our applications may have terms and conditions that describe other privacy commitments or choices in addition to those in this Privacy Policy.

Some areas outside the United States require us to work a little differently. In that case, we may adopt separate privacy policies as necessary to reflect the requirements of applicable local laws.

The Joint AT&T EchoStar Privacy Policy for AT&T/DISH Network Customer Account Information remains in effect for AT&T/DISH subscribers.

4. What about my family members and other users of my AT&T account? Does this Policy apply to them?

Yes. You're responsible for making sure all family members or other users under your account understand and agree to this Policy. Get everyone together and talk about it. Or, send it by e-mail to make sure they're on board. Hang it on the fridge. Up to you, just share it!

5. When is information not covered by this Policy?

If you purchase or use the products or services of an AT&T affiliate that has a different privacy policy than this one, that privacy policy will apply.

Additionally, this Privacy Policy does not apply any time you give information to companies other than AT&T. Some examples are:

- When you use a non-AT&T Wi-Fi service;
- When you download applications or make purchases from other companies while using our Internet or wireless services;
- When you go to a non-AT&T website from one of our websites or applications (by clicking on a link or an advertisement, for example);
- When you give your information to another company through a website co-branded by AT&T but controlled by the other company;
- If you use public forums - such as social networking services, Internet bulletin boards, chat rooms, or blogs - the information is publicly available, and we cannot prevent distribution and use of that information by other parties;
- Information about your location, usage and the numbers you dial when you're out and about and roaming on the network of another company;
- When you purchase or use non-AT&T products (such as wireless devices, internet browsers and mobile applications) in combination with our services;
- When we license our brand to other companies for their use in marketing and selling certain non-AT&T products and services, information you give those companies is not covered by this Policy.

6. Can my information be covered by this Policy and other privacy policies at the same time?

Yes, that can happen. For example:

Sometimes we will work with other, unaffiliated companies to provide a service. In that case your information may be subject to this Policy and that of the other company. For example, you purchase one of our products or services from a retailer like Best Buy or Amazon.com, any information you provide to them may be subject to both their policy and ours.

If you connect to our Wi-Fi service through another network, such as one provided in a hotel, airport or other venue, any information collected from your use of that network could be subject to either the AT&T Privacy Policy or the venue policy, and sometimes both. The same thing applies if you connect to our network through your employer's corporate network, or any network operated by a non-AT&T company.

We think it's a great idea to take a look at the privacy policies of any companies you do business with to learn how they use your information.

7. What about business customers?

We may have written product or service agreements with our business customers that contain specific provisions about confidentiality, security or handling of information. When one of these agreements differs from or conflicts with this Policy, the terms of those agreements will apply. In all other instances, the terms of this Policy apply.

Back to Top.

Questions About The Information We Collect, How We Collect It, And How We Use It**1. What information do you collect?**

We may collect different types of information based on your use of our products and services and on our business relationship with you.

- **Account Information:**
 - **Contact Information** that allows us to communicate with you. We get this information when you order or register for our services. This would include information like your name, address, telephone number and e-mail address.
 - **Billing Information** related to your financial relationship with us, such as the services we provide to you, the telephone numbers you call and text, your payment history, your credit history, your credit card numbers, Social Security number, security codes and your service history.

- **Technical & Usage Information** related to the services we provide to you, including information about how you use our networks, services, products or websites. Some examples include:
 - **Equipment Information** that identifies the equipment on our networks, such as equipment type, device identifiers, device status, serial numbers, settings, configuration and software.
 - **Network Performance & Usage Information** about the operation of the equipment, services and applications you use on our networks. Examples of this might include wireless device location, the number of text messages sent and received, voice minutes used, calling and texting records, bandwidth used, and resources you use when uploading, downloading or streaming data to and from the Internet. We also collect information like transmission rates and delays, data associated with remote monitoring services and security characteristics.
 - Some Network Performance & Usage Information and some Billing Information is **Customer Proprietary Network Information** or "CPNI." Unique rules apply to CPNI. **Go here (/sites/privacy_policy/rights_choices#cpni)** to learn more about what it is, how we use it and the choice you can make about that use.
 - **Web Browsing & Mobile Application Information** such as IP addresses, URLs, data transmission rates and delays. We also learn about the pages you visit, the time you spend, the links or advertisements you see and follow, the search terms you enter, how often you open an application, how long you spend using the app and other similar information.
- **Location Information** includes your ZIP-code and street address, as well as the whereabouts of your wireless device. Location information is generated when your device communicates with cell towers, Wi-Fi routers or access points and/or with other technologies, including the satellites that comprise the Global Positioning System.
- **TV Viewing Information** is generated by your use of any of our satellite or IPTV (U-verse) services. These services may include video on demand, pay per view, DVR services, applications to watch your TV on the go for tablet or smartphone (such as the TV Everywhere app) and similar AT&T services and products, including the programs and channels you and those in your household watch and record, the times you watch and how long you watch. It also includes information like the interactive channels and games provided by U-verse or DIRECTV. We also collect information related to your use and interaction with the equipment in your home, including the TV receivers, set top boxes, remotes and other devices you may use to access our services.

2. How Do You Collect Information?

In three basic ways:

- **You Give It To Us** when you make a purchase or set up an account with us;
- **We Automatically Collect Information** when you use our networks, products and services. For example, we use network tools to collect your call records; we collect wireless device location from our networks and from your device; and we also use **cookies** (/sites/privacy_policy/cookies_and_other_technologies), web server logs and other technologies.
- **We Obtain Information from Outside Sources** like credit reports, marketing mailing lists, and commercially available geographic and demographic information along with other publicly available information, such as public posts to social networking sites.

3. How Do You Use This Information?

We use your information to improve your experience and to make our business stronger. Some examples include:

- Providing and managing your services, responding to your questions and addressing problems;
- Delivering customized content, or advertising, such as personalized offers for products and services that may be of interest to you;
- Communicating service updates, offers and promotions;
- Protecting network integrity and security, ensuring quality control, optimizing capacity and preventing misuse;
- Network enhancement planning, engineering and technical support;
- Conducting research and analysis for maintaining, protecting and developing our networks and our services;
- Preventing illegal activities, suspected fraud, and potential threats to our networks and our customers' networks;
- Investigating violations of our Terms of Service, Acceptable Use Policies, or other service conditions or restrictions; and
- Protecting the safety of any person.

4. Do you use the information I store using one of your cloud services?

We only use it to provide you with that service, unless we first get your permission to use it for something different.

[Back to Top](#)

Questions About Information Sharing

1. Do you provide information for phone books and Caller ID?

Yes and No.

Yes, we share the names, addresses and telephone numbers of our wireline telephone and U-verse Voice customers with businesses that publish directories and provide directory assistance services. We are required by law to do that. You may **contact us** (http://about.att.com/sites/privacy_policy/terms#contact) and we honor your request for non-published or non-listed phone numbers. Once we provide published listing information to those businesses, they may use, sort, package, repackage and make it available again in different formats to anyone.

Yes, we also provide wireline and wireless calling name and number information for CallerID, and related services like Call Trace, which allow a person receiving a call to obtain the name and number of the party calling them.

No, we do not give listing information for wireless numbers to phone book publishers or directory assistance services without your permission.

2. Do you share my Personal Information internally?

Yes. Our products and services are developed, managed, marketed and sold by a variety of our affiliated companies. We may share Personal Information internally, including with affiliated companies that may have different privacy policies. When we do this we require the affiliated company or companies to protect the Personal Information in a way consistent with this Privacy Policy. We may also combine Personal Information with data derived from an application that has a different privacy policy. When we do that, this Privacy Policy applies to the combined data set. Sharing information in these ways helps us offer you the high quality, seamless and innovative range of products you have come to expect from us. Some of these include:

- Wireless voice, data, Internet, home security, automation and remote monitoring services provided by AT&T Mobility and AT&T Digital Life; and
- The suite of satellite and IPTV services, Voice and High Speed Internet Access services offered by our companies.

If one of our subsidiaries does not operate under the AT&T brand, information sharing with that subsidiary is handled as though it is a non-AT&T company.

3. Do you share my Personal Information with other non-AT&T companies for them to market to me?

We will only share your Personal Information with other non-AT&T companies for them to use for the marketing of their own products and services when we have your consent.

4. Are there any other times when you might provide my Personal Information to other non-AT&T companies or entities?

Yes. We share your Personal Information with other, non-AT&T companies that perform services for us, like processing your bill. Because we take our responsibility to safeguard your Personal Information seriously, we do not allow those companies to use it for any purpose other than to perform those services, and we require them to protect it in a way consistent with this Privacy Policy. Companies that perform these services may be located outside the United States or the jurisdiction where you reside. If your Personal Information is shared with these companies, it could be accessible to government authorities according to the laws that govern those jurisdictions. There are also occasions when we provide Personal Information to other non-AT&T companies or other entities, such as government agencies, credit bureaus and collection agencies, without your consent. Some examples include sharing to:

- Comply with court orders, subpoenas, lawful discovery requests and other legal or regulatory requirements, and to enforce our legal rights or defend against legal claims;
- Obtain payment or make refunds for products and services that appear on your AT&T billing statements, including the transfer or sale of delinquent accounts or refund obligations to third parties for collection or payment.
- Enforce our agreements and protect our rights or property;
- Assist with identity verification and e-mail address validation;
- Respond to lawful requests by public authorities, including to meet national security or law enforcement requirements;
- Notify, respond or provide information (including location information) to a responsible governmental entity in emergency or exigent circumstances or in situations involving immediate danger of death or serious physical injury; and
- Notify the National Center for Missing and Exploited Children of information concerning child pornography of which we become aware through the provision of our services.

5. Do you share my personally identifiable TV Viewing Information with other, non-AT&T companies?

We don't share your personally identifiable TV Viewing Information with other non-AT&T companies for them to use for the marketing of their own products and services without your consent. We are required to notify you about the special requirements we must follow when it comes to sharing your personally identifiable TV Viewing Information in response to a Court Order:

Notice Regarding Disclosure of Personally Identifiable Information of Satellite and IPTV Subscribers in Response to A Court Order

- In the case of a court order obtained by a non-governmental entity, we are authorized to disclose personally identifiable information collected from TV subscribers as a result of the subscriber's use of TV service only after providing prior notice to the subscriber.
- In the case of a court order obtained by a governmental entity, we are authorized to disclose personally identifiable information collected from TV subscribers as a result of the subscriber's use of TV service only if, in the court proceeding relevant to the order:
 - The governmental entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and
 - The subject of the information has an opportunity to appear and contest the governmental entity's claim; and
 - We have provided notice to the subscriber as required by applicable state law.

Back to Top

Questions About My Information and Advertising

1. Do you use my information to send me advertising?

Yes. We may use information like the preferences you have expressed and interests you have demonstrated on our websites, in our stores and through use of our products and services, to provide you with marketing information and advertisements for our products and services. Those ads may be delivered on our websites and mobile applications. This is called "first party" advertising. It is part of our service relationship and you are not able to opt-out from this type of advertising.

We or our advertising partners may use **anonymous information gathered through cookies and similar technologies (/sites/privacy_policy/cookies_and_other_technologies)**, as well as other anonymous and aggregate information that either of us may have to help us tailor the ads you see on non-AT&T sites. For example, if you see an ad from us on a non-AT&T sports-related website, you may later receive an ad for sporting equipment delivered by us on a different website. This is called Online Behavioral Advertising, which is a type of Relevant Advertising.

2. Do you use my information for other types of Relevant Advertising?

Yes. We may also use information we get through your use of our products and services, from our advertising partners, and information like your age and gender to deliver Relevant Advertising that is not Online Behavioral Advertising. We combine your anonymous information with that of other users into aggregate "audience segments". These segments are based on particular interests and/or factual characteristics that everyone in that audience segment is likely to share. We might use that information to send you advertisements that are relevant to those interests or characteristics. We are careful to only use non-personally identifiable information to create Relevant Advertising with aggregate audience segments that are large enough that you can't be identified individually.

In some cases you may agree to participate in advertising offers or programs through loyalty programs, when you download a mobile app, or other similar programs. In those cases, you will be told about the advertising program when you sign up. For more information about those advertising programs, please consult the terms, conditions, and policies of the specific application or loyalty programs you are interested in or have joined.

3. Do you use the location of my device for advertising purposes?

Yes. We use information about the locations you visit in order to create combined wireless location interest characteristics that can be used to provide Relevant Advertising to you and others like you.

Location characteristics are types of locations - like "movie theaters". People who live in a particular geographic area (a city, ZIP-code or ZIP+ 4 code, for example) might appear to have a high interest in movies, thanks to collective information that shows wireless devices from that area are often located in the vicinity of movie theaters. We might create a "movies characteristic" for that area, and deliver movie ads to the people who live there.

We may associate your wireless device with a particular geographic area, such as a city, ZIP-code, or ZIP + 4 code, based on your billing address or the cell towers you connect with most frequently.

In addition to other privacy protections, the process we use to create our audience segment includes a requirement that the ZIP + 4 or other geographic area to which a wireless location is assigned must contain a minimum of 25 households. ZIP + 4 codes with less than 25 households are combined with other ZIP + 4 codes to satisfy this requirement.

4. What's in it for me?

Just like the name says, you get advertising that's more relevant to your interests. For example, if a particular audience segment, like adults between the ages of 21 and 25 with a certain income range, has demonstrated a greater interest in movies than other segments, we might send them a movie ad for a movie geared toward young adults. This is just one way we deliver content that's more relevant.

5. How do you use information about the programs I watch on TV to advertise to me?

We combine information about the shows that our customers are watching with their common interests to help us figure out what types of advertising they might be interested in seeing.

It sometimes works like this: We look at the group of people watching a particular show. We identify common characteristics within that group. We use those characteristics to identify and deliver advertising that might be most relevant to watchers of that TV show. We might also deliver that same advertising during shows that appear to have similar audiences.

6. Do I ever have a chance to tell you what I'm personally interested in?

Yes. With some programs offered or powered by AT&T you can sign up to receive text-message offers from businesses that are near your current location and match the interests you've selected. You can change your mind at any time and stop participating in these programs.

7. What information do you provide to advertisers?

We may provide reports to advertisers and other business customers about the success of its advertising campaigns. Those reports contain aggregate information about the number of times a particular ad was viewed, when it was viewed, whether it was viewed on a TV, a mobile device or a computer, demographics associated with the viewing audience and other similar information. Your anonymous information will not be included in aggregate reports about the success of Relevant Advertising campaigns if you have opted-out of Relevant Advertising delivered by AT&T.

Back to Top

Questions About Location Information

1. What is location information?

Exactly what it sounds like! It includes your ZIP-code and street address, as well as the whereabouts of your wireless device.

2. How is it used?

We use it in all kinds of ways, here are some examples:

- **We Provide Wireless Voice and Data Services:** We monitor, collect and use wireless location information, together with other information we get from our network and your wireless device, to maintain and improve our network. We also might use location information with your consent to provide you with a customized experience. For example, when you dial 411 Directory Assistance for a business telephone number, we might use your wireless location information to return the number of the business location closest to you.
- **Location Based Services (LBS):** Your device can be used to access a ton of services based on location. We offer these services via applications that have been pre-loaded or downloaded by you on your device. LBS also may be provided via text message or other functionality. We'll give you prior notice and ask for your consent when your location is used or shared. The form of consent may vary, but will be appropriate for the type of LBS you use.
- **LBS from other providers:** With your consent (to us or the other company) we also may enable LBS from other companies by providing location information to their developers or location service providers.
- We use it for **Advertising**

3. How accurate is wireless location information?

It depends on the technology we're using. For example, we can locate your device based on the cell tower that's serving you. The range could be up to 1,000 meters in any direction from the tower in urban areas, and up to 10,000 meters in rural areas. Wi-Fi networks provide more accurate location information, associating you with the place where the network is located - like a coffee shop - or to an area within or around that place.

Services such as 411, 911, a "friend locator" application or a navigation/mapping application, require more precise information. So for those we develop a more precise estimate of location by associating the serving cell tower ID with other information, like the latitude and longitude of the tower, radio frequency parameters, GPS information and timing differences in radio signals. Depending on a variety of factors, those methods may estimate the location of your device to within 30 to 1000 meters.

4. Are you the only ones who can locate my wireless device?

Other companies may also be able to locate your device. For example, your handset manufacturer and your operating system provider may be able to locate your device. If you download mobile applications, those apps may be able to obtain your location directly from your handset or the operating system. Mobile applications that give you access to your employer's network may also give your employer the ability to locate your device.

We urge you to review policies of all providers.

Back to Top

Questions About Aggregate and Anonymous Information**1. Where do you get anonymous information?**

Sometimes we'll collect information about how you use our products **using cookies and other similar technologies (/sites/privacy_policy/cookies_and_other_technologies)**. This information doesn't include your Personal Information and is considered anonymous.

When we collect information that identifies you personally, we may anonymize it for certain purposes. We remove data fields (such as name, address and telephone number) that can reasonably be used to identify you. We also use a variety of statistical techniques and operational controls to anonymize data. Anonymizing information is one of the tools we use to protect your privacy.

2. Tell me more about aggregate information.

Aggregate information is a form of anonymous information. We combine data that meet certain criteria into anonymous groups. For example, we might want to compare how customers in Beverly Hills, CA (or any city, county or ZIP-code) use their cell phones to how customers in Boulder, CO use their cell phones. In order to do that, we would combine customer data in each of the geographies into anonymous groups and look at all that aggregate data to understand how the two groups are different or similar.

3. Do you share anonymous or aggregate information?

Yes, we may share this information with other companies and entities for specific uses, which may include:

- Universities, laboratories, think tanks and other entities that conduct networking, social, behavioral, environmental and other types of scientific research, for the purpose of creating fundamental new knowledge;
- Municipalities, government or other entities that may use this data for purposes such as municipal and transportation planning, and emergency and disaster response coordination.

We share this information in external reports like our External Marketing & Analytics Reports and Metric Reports.

Back to Top

Questions About External Marketing & Analytics Reports**1. Tell me more about the External Marketing & Analytics Program.**

We use aggregate information to create External Marketing & Analytics Reports that we may sell to other companies for their own marketing, advertising or other similar uses.

These reports may be a combination of information from wireless and Wi-Fi locations, TV Viewing, calling and texting records, website browsing and mobile application usage and other information we have about you and other customers. You have a choice about whether your anonymous information is included in the reports that we sell or provide to other companies.

Some examples of External Marketing & Analytics Reports include:

- Reports for retail businesses that show the number of wireless devices in or near their store locations by time of day and day of the week, together with demographic characteristics or other information about the users (such as device type, age or gender) in those groups.
- Reports that combine anonymous TV Viewing behaviors with other aggregate information we may have about our subscribers to create reports that would help a TV network better understand the audiences that are viewing their programs, those that are not, how frequently they watch, when they watch and other similar information; and
- Reports for device manufacturers that combine information such as device type, make and model with demographic and regional location information to reflect the popularity of particular device types with various customer segments.

2. Do you provide companies with individual anonymous data as part of your External Marketing & Analytics Program?

Yes. For example, we might share anonymous TV Viewing Information with media research companies that combine this data with other information to provide audience analysis services about what shows certain audience segments are watching. When we provide individual anonymous information to businesses, we require that they only use it to compile aggregate reports, and for no other purpose. We also require businesses to agree they will not attempt to identify any person using this information, and that they will handle it in a secure manner, consistent with this Policy.

3. Do you use my anonymous information in other types of external reports?

Yes, we may use your anonymous information to provide Metrics Reports to our business customers and service suppliers. These reports are considered part of the underlying service and we do not sell them to other customers or suppliers.

For example, if you connect to our Wi-Fi service in a hotel, airport or other venue you should know the operator of that venue is our business customer, and that we will provide that operator with Metrics Reports about usage of and communications with the Wi-Fi network in their location. Those reports contain statistical information like:

- The number of devices connecting to the Wi-Fi network, duration of Wi-Fi sessions and the amount of bandwidth used during those sessions; and
- Foot-traffic data, including the numbers of devices inside and outside the store at a given time; the number of new and frequent visitors; where visitors are located within the store (e.g., specific departments or other locations within the venue) and frequency of visits and time spent within the store.
- **NOTE:** When your wireless device is turned on, it regularly sends out signals that enable it to connect to cell towers, Wi-Fi access points or other technologies so that we (and others) are able to provide you with services. These signals can be used to determine your device location. You can turn Wi-Fi to the "off" position on the "settings" feature of your device to prevent the collection of these signals by Wi-Fi equipment in retail stores and other public places.

Another example, we also license video programming from content providers. As part of our agreement, we provide them with Metrics Reports. These reports contain combined measurements and statistical information related to the number of TV subscribers who watched or accessed a particular program at a particular time and other similar measurements.

Back to Top

Questions About Our Online Privacy Policy for Children

1. Do you collect information about my children's use?

We do not knowingly collect personally identifying information from anyone under the age of 13 unless we first obtain permission from the child's parent or legal guardian.

2. What happens when my child is using an account not registered to them?

Internet and wireless devices and services purchased for family use may be used by children without our knowledge. When that happens, information collected may appear to us to be associated with the adult customer who subscribes to our services and will be treated as the adult's information under this Policy.

3. What can I do to help better protect my child's information?

We encourage you to spend time online with your children, and to participate in and monitor their online activity. We have developed a website that offers safety and control tools, expert resources and tips designed to help you manage technology choices and address safety concerns. Please visit **AT&T Smart Controls** (<https://www.att.com/shop/wireless/smartcontrols.html>) for more information.

4. What if my child has an AT&T e-mail sub-account?

If you create an AT&T e-mail sub-account for a child under the age of 13:

- With your permission we collect your child's name, nicknames and aliases, alternative e-mail address, birth date, gender and ZIP-code.
- We use the information collected on sub-accounts to create and maintain those accounts, for research, to customize the advertising and content seen on our pages and for other marketing purposes. Your child can use their AT&T e-mail address and password to log onto websites and online services provided by us, like uverse.com (<http://uverse.com/>). We and our advertising partners may collect and use information about customers who log onto those sites as described in the "Questions about the Information We Collect, How we Collect It and How We Use It" section of this Privacy Policy. A

list of the advertising partners who collect information on our sites and the ability to opt-out of advertising provided by those partners is available [here \(/sites/privacy_policy/rights_choices\)](#).

- We will not contact a child under the age of 13 about special offers or for marketing purposes without parental consent.
- You or your child can review, edit, update, and delete information relating to your child's sub-account and, if you no longer wish your child to have such an account, you can revoke your consent at any time, by logging on to manage your account [here \(https://www.att.com/olam/loginAction.olamexecute?actionType=manage\)](https://www.att.com/olam/loginAction.olamexecute?actionType=manage).

You may e-mail us at privacypolicy@att.com (<mailto:privacypolicy@att.com>), call us at 800.495.1547 or write to us at AT&T Privacy Policy, Chief Privacy Office, 208 S. Akard, Room 1033, Dallas, TX 75202 with any questions or concerns you may have about our Children's Online Privacy Policy.

Back to Top

Questions About Data Protection & Security

1. Do we sell your Personal Information?

No. We do not sell your **Personal Information (/sites/privacy_policy/terms#definitions)** to anyone, for any purpose. Period.

2. How long do we keep your Personal Information?

We keep your **Personal Information (/sites/privacy_policy/terms#definitions)** as long as we need it for business, tax or legal purposes. After that, we destroy it by making it unreadable or undecipherable.

3. What safeguards does AT&T have in place?

We've worked hard to protect your information. And we've established electronic and administrative safeguards designed to make the information we collect secure. Some examples of those safeguards include:

- All of our employees are subject to the **AT&T Code of Business Conduct (COBC)** (https://www.att.com/Common/about_us/downloads/att_code_of_business_conduct.pdf) and certain state-mandated codes of conduct. Under the COBC, all employees must follow the laws, rules, regulations, court and/or administrative orders that apply to our business - including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of your records. We take this seriously, and any of our employees who fail to meet the standards we've set in the COBC are subject to disciplinary action. That includes dismissal.
- We've implemented technology and security features and strict policy guidelines to safeguard the privacy of your **Personal Information**. Some examples are:
 - Maintaining and protecting the security of computer storage and network equipment, and using our security procedures that require employee user names and passwords to access sensitive data;
 - Applying encryption or other appropriate security controls to protect **Personal Information** when stored or transmitted by us;
 - Limiting access to **Personal Information** to only those with jobs requiring such access; and
 - Requiring caller/online authentication before providing **Account Information** so that only you or someone who knows your **Account Information** will be able to access or change the information.
 - Although we strive to keep your **Personal Information** secure, no security measures are perfect, and we cannot guarantee that your **Personal Information** will never be disclosed in a manner inconsistent with this Policy (for example, as the result of unauthorized acts by third parties that violate the law or this Policy).

4. Will you notify me in case of a security breach?

Laws and regulations guide us in how to give you notification when certain types of sensitive information are involved in a security breach. We will provide you with notice in accordance with these laws and regulations.

5. Can I review and correct my Personal Information?

Yes. We are happy to help you review and correct the **Personal Information** we have associated with your account and billing records within a reasonable time. Please see the **How to Contact Us About This Policy** (http://about.att.com/sites/privacy_policy/terms#contact) section.

Back to Top

Questions About Future Changes

1. What happens if there is a change in corporate ownership?

Information about our customers and users, including Personal Information, may be shared and transferred as part of any merger, acquisition, sale of company assets or transition of service to another provider. This also applies in the unlikely event of an insolvency, bankruptcy or receivership in which customer and user records would be transferred to another entity as a result of such a proceeding.


2. Will I be notified if there are changes to this policy?

We may update this Privacy Policy as necessary to reflect changes we make and to satisfy legal requirements. We will post a prominent notice of material changes on our websites. We will provide you with other appropriate notice of important changes at least 30 days before the effective date.

Back to Top

Your Choices & Controls

1. You can choose not to receive some types of advertising online, on your satellite TV service or on your wireless device.

- **Relevant Advertising:** Opt-out of Relevant Advertising delivered by AT&T [here](https://cprodmasx.att.com/commonLogin/igate_wam/controller.do?TAM_OP=login&USERNAME=unauthenticated&ERROR_CODE=0x00000000&ERROR_TEXT=HPDBA0521I%20%20%20Success) (https://cprodmasx.att.com/commonLogin/igate_wam/controller.do?TAM_OP=login&USERNAME=unauthenticated&ERROR_CODE=0x00000000&ERROR_TEXT=HPDBA0521I%20%20%20Success)
- **Online Behavioral Advertising:** Advertising that is customized based on predictions generated from your visits over time and across different websites is sometimes called "online behavioral" or "interest-based" advertising. In accordance with industry self-regulatory principles, you can opt out of online behavioral advertising from companies who participate in the **Digital Advertising Alliance** (<http://www.aboutads.info/>) by going to their **Consumer Choice Page** (<http://www.aboutads.info/choices/#completed>) or by clicking on this icon  (<http://www.aboutads.info/>) when you see it on an online ad. Opt-out of online behavioral advertising from many other ad networks at the **Network Advertising Initiative (NAI)** site (<http://www.networkadvertising.org/choices/>).
- **Information about Cookies and Similar Technologies:** To limit collection of data on web sites that may be used for advertising, go [here](http://about.att.com/sites/privacy_policy/cookies_and_other_technologies) (http://about.att.com/sites/privacy_policy/cookies_and_other_technologies) for information on how to manage cookies and other similar technologies on your computer.
- **Advertising on att.net:** Opt-out of receiving interest-based advertising when using our att.net portal services powered by Synacor (<http://www.aboutads.info/choices>). Opt-out of interest-based advertising on att.net from Yahoo! This covers att.net email and also the Yahoo! (<https://aim.yahoo.com/aim/us/en/optout/index.htm>) portal that is being retired.
- **Advertising Offers from Apps and Loyalty Programs:** In some cases you may agree to participate in advertising offers or programs through loyalty programs, when you download a mobile app, or other similar programs. For example, if you have the DIRECTV app, you can find out more about your choices concerning how your DIRECTV viewing information is used and shared [here](https://www.directv.com/DTVAPP/content/support/DTVAPP_policy) (https://www.directv.com/DTVAPP/content/support/DTVAPP_policy).

2. Do I have choices about receiving first party advertisements from AT&T?

Because first party advertising is part of the service you receive when you visit our websites and use our mobile applications, we don't offer an opt-out for first party advertising.

3. Can I choose not to receive marketing and other types of communication from AT&T?

We realize that unwanted marketing contacts can be a hassle and we've worked hard to meet the expectations of customers and potential customers who have expressed a desire to limit certain types of solicitation communications from us.

E-Mail: Every marketing e-mail we send contains instructions and a link that will allow you to stop additional marketing e-mails for that product or service type. You also can unsubscribe from AT&T marketing e-mails **here** (<http://www.att.com/remove>).

Text Messages: Opt-out of AT&T marketing text message contacts by replying "stop" to any message.

AT&T Consumer Telemarketing: Ask to be removed from our consumer telemarketing lists by contacting us at **one of the numbers listed here** ([/sites/privacy_policy/rights_choices#cpnicontact](https://www.att.com/sites/privacy_policy/rights_choices#cpnicontact)). You also can ask the AT&T representative to remove you from our telemarketing lists when you receive a marketing or promotional call from us.

AT&T Business Telemarketing: Where required by local laws and/or regulations, we honor requests to be removed from our telemarketing lists from business customers.

Federal Do Not Call: The FTC maintains a National Do Not Call Registry at [donotcall.gov](http://www.donotcall.gov) (<http://www.donotcall.gov>), and some states in the United States may maintain its own Do Not Call Registry. Putting your number on these Registries also may limit our AT&T telemarketing calls to that number.

Postal Mail: To review our Residential Do Not Mail Policy Statement and to limit postal mail solicitations, click **here** ([/sites/privacy_policy/att_consumer_marketing](https://www.att.com/sites/privacy_policy/att_consumer_marketing)). You will still receive billing statements, legal notices, product updates and other similar correspondence, and you may still receive some promotional mailings.

All of our practices are designed to satisfy state, provincial and federal legal requirements limiting marketing contacts. Those laws and regulations - such as the requirements governing the state and federal "Do Not Call" lists - generally permit companies to contact their own current and, in some cases, former customers, even when those customers are listed on the federal and state "Do Not Call" lists.

Automated Calls or Messages: In some cases, we will ask for your permission to send you automated calls or messages to your mobile phone. To opt out of these calls or messages from AT&T, please go to **Manage Your Privacy Choices** (<http://www.att.com/cmpchoice>). As required or allowed by law, even if you opt out, AT&T may continue to contact you with automated calls or messages at the telephone number issued by us for certain important informational messages about your service. For example, we may need to let you know about a problem with your wireless service.

Restricting our use of your CPNI will not eliminate all types of our marketing contacts.

4. Can I choose to exclude my anonymous information from your External Marketing & Analytics and other similar reports?

Yes. Click **here** (<https://www.att.com/cmpchoice>) to opt-out. This opt-out also applies to the sharing of your anonymous information with other companies for their use in creating marketing and analytics reports. Although this opt out does not apply to Metrics Reports, it will apply if we combine Metrics Report information with other customer information (like demographics) to create reports that we provide to our business customers or service suppliers.

5. What is DNS error assist?

When you mistype a web address, or the address is not working, DNS Error Assist provides an automated list of similar pages - such as possibly the one you meant to type - for your consideration. The service is provided on your AT&T residential broadband connection, and you can opt-out **here** (<http://www.att.com/cmpchoice>). If you opt-out, you will get a standard "no results found" error message instead of the error-assist page.

6. Are there any other opt-out choices I should know about?

We may use services provided by analytics companies to obtain information about website performance and how you use our mobile applications and other products and services. **Go here** (<http://www.aboutads.info/choices/>) for more information about the opt-outs made available by some of those vendors, and to make choices about participation. Based on your permission, we may share your mobile device location or other mobile subscriber information with third parties when you use Third-Party Services, such as to prevent fraud when making a bank transaction. If you want to change that permission, you can opt out directly with the third party or you can opt out by going to Manage Your Privacy Choices.

7. These Choices and Controls also are available at [http://about.att.com/sites/privacy_policy/rights_choices\(/sites/privacy_policy/rights_choices\)](http://about.att.com/sites/privacy_policy/rights_choices(/sites/privacy_policy/rights_choices)).

Back to Top

How to Contact Us About This Policy

We encourage you to contact us directly at either of these addresses below for any questions about this Privacy Policy.

- E-mail us at privacypolicy@att.com (<mailto:privacypolicy@att.com>)
- Write to us at AT&T Privacy Policy, Chief Privacy Office, 208 S. Akard, Room 1033, Dallas, TX 75202.

For questions not related to privacy click on the "Contact Us" link at the bottom of any **att.com** (<http://www.att.com/>) page. You also can access your online account from the upper right hand corner of our home page at att.com for additional service options.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, you may contact our U.S.-based third-party ombudsperson program at <https://www.truste.com/consumer-resources/dispute-resolution/dispute-resolution-faqs/> (<https://www.truste.com/consumer-resources/dispute-resolution/dispute-resolution-faqs/>). If you are not satisfied with our resolution of any dispute, including with respect to privacy or data use concerns, please review our dispute resolution procedures at <http://www.att.com/disputeresolution> (<http://www.att.com/disputeresolution>).

You also have the option of filing a complaint with the FTC Bureau of Consumer Protection, using an **online form** (<https://www.ftccomplaintassistant.gov>), or by calling toll-free 877.FTC.HELP (877.328.4357; TTY: 866.653.4261). Other rights and remedies also may be available to you under federal or other applicable laws.

If you are a satellite TV subscriber, you also have certain rights under **Section 338(i) of the Federal Communications Act** (<http://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/pdf/USCODE-2011-title47-chap5-subchapIII-partI-sec338.pdf>).

If you are a DIRECTV customer in Puerto Rico, you can exercise and manage your choices by visiting <https://www.directvpr.com/Midirectv/ingresar> (<https://www.directvpr.com/Midirectv/ingresar>) or by calling 787-776-5252.

Back to Top

Customer Proprietary Network Information (CPNI)

What is CPNI?

"CPNI" is information about your phone service from us. Your phone service could be a cell phone or any sort of home or business phone. The "information" is things like what kind of services you have, how you use them, or billing information. (Your telephone number, name and address are not considered CPNI.)

Back to Top

How is CPNI Used and Disclosed?

We do not sell, trade or share your CPNI with anyone outside of the AT&T family of companies* or our authorized agents, unless required by law (example: a court order).

We do use your CPNI internally, however. We may share information about our customers among the AT&T companies and our agents in order to offer you new or enhanced services. For example, we might offer a discount or promotion for Internet or TV services based on your CPNI.

Back to Top

How may I limit the use of my CPNI?

AT&T uses technology and security features, and strict policy guidelines with ourselves and our agents, to safeguard the privacy of CPNI. It is your right and our duty under federal law to protect the confidentiality of your CPNI.

If you don't want AT&T to use your CPNI internally for things like offers, here is what you can do:

You can "opt out" online, at att.com/ecpniptout (<http://att.com/ecpniptout>), or

You can call 800.315.8303, any time of day, and follow the prompts, or

You can speak to a service representative at 800.288.2020 (consumer) or 800.321.2000 (business).

For languages other than English and Spanish, please visit world.att.com (<http://world.att.com>).

If you choose to restrict our use of your CPNI, it won't affect any of your services. You can change your mind at any time about allowing (or not allowing) us to use your CPNI, and we'll honor your decision until you change it again. If you do restrict your CPNI use, you may still get marketing from us, but it won't be from using CPNI.

** The AT&T Family of Companies are those companies that provide voice, video and broadband-related products and/or services domestically and internationally, including the AT&T local and long distance companies, AT&T Corp., AT&T Mobility, DIRECTV, and other subsidiaries or affiliates of AT&T Inc. that provide, design, market, or sell these products and/or services.*

Back to Top

Customer Service Contact Numbers

Wireless - 1-800-331-0500

Business - 1-800-321-2000

Residential - 1-800-288-2020

Spanish Language - 1-800-870-5855

Satellite TV Services - 1-800-DIRECTV or 1-800-531-5000

For assistance in other languages, please visit world.att.com (<http://world.att.com>).

Legacy AT&T Consumer - 1-800-222-0300

Customers of the following AT&T family of companies may contact us directly using the following:

AT&T Internet Services - Customers can manage newsletter subscriptions or other e-mail communications from Yahoo! by modifying their AT&T Yahoo! Marketing Preferences.

Back to Top

EXHIBIT “C”

A Conversation with Randall Stephenson and David Huntley: Code of Business Conduct

Why is it important for us to have a Code of Business Conduct?

Stephenson: We're guided by a core set of values at AT&T. That's who we are. These values guide our mission, which is what we're all about. And our strategy is how we fulfill that mission. The Code of Business Conduct is the codification of our core values. It lays out the guidelines and expectations for how we do business, how we operate, and how we interact with customers, suppliers, owners, and each other. We hold ourselves to the highest standards. That means always doing the right thing. And it means operating with integrity, transparency, and honesty in everything we do.

What does our Code of Business Conduct mean to our employees?

Huntley: Our customers count on us. They count on us to create the best entertainment and communications experiences in the world. And that requires an environment of trust from all employees at AT&T. Trust that we will protect their information. That we will do what we say. That we will follow not only the letter of the law, but the spirit of the law. And that we will always take responsibility. When our employees do those things, we protect our brand and we respect our customers. And that makes us a stronger company and a great place to work. Our interactive Code of Business Conduct, available on your desktop or mobile device, empowers employees to take personal ownership of an ethical culture here at AT&T.

How does our Code of Business Conduct align with where we're headed as a company?

Stephenson: Our business has changed radically over the years. And it will continue to change as we become a global leader in telecom, media, and technology. But what will never change is our commitment to our core values and the Code of Business Conduct. Consistently following the Code and doing the right thing has never been more important. It's the foundation of who we are.

Code of Business Conduct: Mission Statement

Our vision at AT&T - connect people with their world, everywhere they live, work, and play, and do it better than anyone else - is what unifies us as a company. In order to fulfill that mission, each of us must take personal responsibility for protecting AT&T's long-standing reputation as an ethical business. Our Code of Business Conduct lays out our commitment to each other, to our customers, to our shareholders, and to all who have a stake in AT&T's success.

While no Code of Business Conduct can provide rules that cover every situation or challenge, ours serves as a guide for each of us. It reinforces our commitment to just do the right thing, and empowers us to take action and make the right decisions, even when they're challenging. By keeping our commitment and making the right decisions, we safeguard AT&T's solid reputation. It is this reputation that enables us to deliver on our mission with the integrity and trust our customers expect.

AT&T Code of Business Conduct

Our Commitment to Our Customers

- ⊕ We follow ethical sales practices.
- ✓ We comply with regulations that apply to government customers.
- ✓ We guard the privacy of our customers' communications.

We protect the privacy of our customers' communications. Not only do our customers demand this, but the law requires it. Consistent with this principle, although we comply with government requests for customer communications, we do so only to the extent required by law. Maintaining the confidentiality of communications is, and always has been, a crucial part of our business.

- ✓ We protect the information about our customers that they entrust to us.

Need more Information?

[COBC PDF](#)[Privacy Policy](#)[Terms of Use](#)[Non-Exempt Employee Notice](#)

English (United States) ▼

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.

AT&T Code of Business Conduct

Our Commitment to Our Customers

- ⊕ We follow ethical sales practices.
- ✓ We comply with regulations that apply to government customers.
- ✓ We guard the privacy of our customers' communications.
- ✓ We protect the information about our customers that they entrust to us.

AT&T possesses sensitive, detailed information about our customers, who rely on AT&T to safeguard that information. Laws and regulations tell us how to treat such data. Any inappropriate use of confidential customer information violates our customers' trust and may also violate a law or regulation. Preserving our customers' trust by safeguarding their private data is essential to our reputation.

Need more Information?

[COBC PDF](#)[Privacy Policy](#)[Terms of Use](#)[Non-Exempt Employee Notice](#)

English (United States) ▼

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.

AT&T Code of Business Conduct

Our Commitment to Our Customers

- ✓ We follow ethical sales practices.
Our customers should always know we value them. We fairly represent our products and services to them. We listen to our customers, and challenge ourselves to find new ways to offer the best solutions available to help them communicate efficiently, sustainably, and safely.
We earn and preserve their trust by treating them with honesty and integrity and in a professional, courteous manner. We deliver what we promise. We do not provide goods or services that customers did not authorize. Sometimes our customers are our competitors and suppliers as well. In those situations, we serve them in the same professional manner we would extend to any customer.
- ✓ We comply with regulations that apply to government customers.
- ✓ We guard the privacy of our customers' communications.
- ✓ We protect the information about our customers that they entrust to us.

Need more Information?

[COBC PDF](#)[Privacy Policy](#)[Terms of Use](#)[Non-Exempt Employee Notice](#)[English \(United States\)](#) ▼

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.

AT&T Code of Business Conduct

Our Commitment to Our Customers

- ✓ We follow ethical sales practices.
- ✓ We comply with regulations that apply to government customers.

Doing business with certain government entities requires adhering to strict and sometimes unique regulations. We are well trained about these rules, and we follow these regulations in our interaction with the government. We are committed to this enhanced level of diligence for these governmental customers. We follow instructions to seek advice immediately from our internal experts whenever we are in doubt about any activity. In particular, dealing with schools, libraries, and rural health care providers imposes strict rules that require special training prior to any activity and require constant diligence.

- ✓ We guard the privacy of our customers' communications.
- ✓ We protect the information about our customers that they entrust to us.

Need more Information?

[COBC PDF](#)[Privacy Policy](#)[Terms of Use](#)[Non-Exempt Employee Notice](#)[English \(United States\)](#) ▼

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.

AT&T Code of Business Conduct

Our Commitment to the Code

- ✓ We respect the Code, and apply it to our work every day.

As AT&T employees, we are part of a long tradition of employees who have conducted themselves in an ethical manner that reflects positively on the Company. We focus on doing the right thing - upholding our shared commitment to complying with laws, regulations, and internal policies. Each employee is responsible for being familiar with the information in this Code and for following the Code and the Company's policies and guidelines. We understand that violations may result in discipline, up to and including termination of employment.

We know that no one has the authority to direct any employee to violate the law, this Code, or AT&T's policies.

This Code applies to all employees of AT&T around the world.

- ⊕ We cooperate with investigations to uphold the Code.
- ⊕ We know our reporting rights and responsibilities.
- ⊕ We do not retaliate.
- ⊕ We know where to find additional guidance.

Need more Information?

[COBC PDF](#)[Privacy Policy](#)[Terms of Use](#)[Non-Exempt Employee Notice](#)

English (United States) ▼

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.

EXHIBIT “D”

WIRELESS CUSTOMER AGREEMENT ("Agreement")

"AT&T" or "we," "us," or "our" refers to AT&T Mobility LLC, acting on behalf of its affiliates doing business as AT&T or other brands owned by AT&T. "You" or "your" refers to the person or entity that is the customer of record.

PLEASE READ THIS AGREEMENT CAREFULLY TO ENSURE THAT YOU UNDERSTAND EACH PROVISION, INCLUDING OUR USE OF YOUR LOCATION INFORMATION (SEE SECTION 3.6). THIS AGREEMENT REQUIRES THE USE OF ARBITRATION ON AN INDIVIDUAL BASIS TO RESOLVE DISPUTES, RATHER THAN JURY TRIALS OR CLASS ACTIONS, AND ALSO LIMITS THE REMEDIES AVAILABLE TO YOU IN THE EVENT OF A DISPUTE.

This Agreement, including the AT&T Privacy Policy Located at att.com/privacy, Customer Service Summary, and terms of service for wireless products, features, applications, and services (including content and other AT&T services included with your wireless service) ("Services") not otherwise described herein that are posted on applicable AT&T websites or devices, and any documents expressly referred to herein or therein, make up the complete agreement between you and AT&T and supersede any and all prior agreements and understandings relating to the subject matter of this Agreement.

AT&T's wireless network may provide broadband access to the Internet. For more information about how AT&T helps transmit information to points on the Internet and how we manage our network, please see the Broadband Information page which can be found at: www.att.com/broadbandinfo.

1.0 TERM COMMITMENT, CHARGES, BILLING AND PAYMENT

1.1 What Is The Term Of My Service? How Can I Fulfill My Service Commitment? What are My Rights to Cancel Service and Terminate My Agreement?

AT&T wireless Service(s) may be used with: (a) a mobile device that contains a SIM that is assigned to your account ("Device") and/or, (b) a device that is designed and purchased for use exclusively on AT&T's network ("Equipment").

Term of Service. Your Agreement begins on the day we activate your Service(s) and continues through the Term of Service, typically a 12 month or 24 month period ("Service Commitment"), specified on your Customer Service Summary. At the end of your service commitment, this Agreement will automatically continue on a month-to-month basis. If your Agreement has no Service Commitment, it is a month-to-month Agreement.

Device Activation. If You purchased a device that was shipped to You, You agree to activate the device within seven (7) days of the shipment date. If Your device is not activated by You, we may activate the device for You within a month of shipping and Your monthly recurring charges, and any applicable Service Commitment, will begin.

Fulfillment of Service Commitment. You have received certain benefits from us in exchange for your Service Commitment, which may include, but are not limited to, a subsidized wireless device. There are two alternative ways to fulfill your Service Commitment. You can pay for the Services described in your Customer Service Summary for the term of your Service Commitment, or you can terminate your Agreement prior to the end of your Service Commitment and pay an Early Termination Fee ("ETF"). The Early Termination Fee is not a penalty, but rather is an alternative means for you to perform your obligations under the Agreement that partially compensates us for the fact that the Service Commitment on which your rate plan is based was not completed.

Your Termination Rights. Within the first 14 days after service activation, you may terminate your Agreement for any reason and not be required to pay an ETF. If you terminate within three (3) days of accepting the Agreement, AT&T will refund your activation fee, if any. However, you agree to pay AT&T for all fees, charges, and other amounts incurred and owed under your Agreement, and you agree to return to AT&T any Equipment you purchased from AT&T in connection with your Service Commitment. If you fail to return this Equipment, you will be charged the difference between the amount you paid AT&T for the Equipment and the amount you would have been charged for the Equipment had you not agreed to a Service Commitment. AT&T also may charge you a restocking fee for any returned Equipment. Some dealers may impose additional fees.

After the first 14 days, you may terminate your Agreement for any reason. However, you agree to pay AT&T for all fees, charges, and other amounts incurred and owed under your Agreement along with the applicable ETF. The Early Termination Fee is either: (a) \$325 or (b) \$150. The ETF reduces each full month of your Service Commitment that you complete. To determine whether your Equipment has a \$325 Early Termination Fee or a \$150 Early Termination Fee, and the amount of reduction, check att.com/equipmentETF.

After your Service Commitment ends and you are on a month-to-month Agreement, you may terminate your Agreement at any time with 30 days notice without incurring an ETF. If you sign a new Agreement before the end of the term of your existing Agreement and terminate that new Agreement within 14 days as allowed above, you agree that you will be bound by the terms and conditions of your existing Agreement including fulfillment of any remaining Service Commitment thereunder.

1.2 What are AT&T's Rights to Cancel My Service(s) and Terminate My Agreement?

AT&T may interrupt, suspend or cancel your Services and terminate your Agreement without advance notice for any reason including, but not limited to, the following:

- Any conduct that we believe violates this Agreement or AT&T's Acceptable Use Policy;

- Any conduct that involves the use of abusive, derogatory, insulting, threatening, vulgar or similarly unreasonable language or behavior directed at any of our employees or representatives whether it be in person, over the phone, or in writing;
- Any abusive use of our network or Services;
- You use your Device/Equipment and/or our Services for an unlawful or fraudulent purpose;
- You use your Device/Equipment and/or our Services in any way that: (a) is harmful to, interferes with, or negatively affects our network, other customers, or the network of any other provider, (b) is harmful to, interferes with, or negatively affects our Services or operations, (c) infringes intellectual property rights of AT&T or others, (d) results in the publication of threatening, offensive or illegal material, or (e) generates spam or other abusive messaging or calling, a security risk, or a violation of privacy;
- You resell our Services either alone or as part of any other good or service;
- You fail to make all required payments when due;
- Your credit has deteriorated and/or we believe that there is a risk of non-payment;
- You refuse to pay any required advance payment or deposit;
- We discover that you are underage;
- You provide inaccurate or misleading credit information; or
- You modify your device from its manufacturer's specifications.

AT&T's rights under this Section 1.2 are in addition to any specific rights that we reserve in other provisions of this Agreement to interrupt, suspend, modify, or cancel your Services and terminate your Agreement.

After your Service Commitment ends and you are on a month-to-month Agreement, AT&T may terminate your Agreement at any time with 30 days notice.

1.3 Can AT&T Change My Terms And Rates?

We may change any terms, conditions, rates, fees, expenses, or charges regarding your Services at any time. We will provide you with notice of material changes (other than changes to governmental fees, proportional charges for governmental mandates, roaming rates or administrative charges) either in your monthly bill or separately. You understand and agree that State and Federal Universal Service Fees and other governmentally imposed fees, whether or not assessed directly upon you, may be increased based upon the government's or our calculations.

IF WE INCREASE THE PRICE OF ANY OF THE SERVICES TO WHICH YOU SUBSCRIBE, BEYOND THE LIMITS SET FORTH IN YOUR CUSTOMER SERVICE SUMMARY, OR IF WE MATERIALLY DECREASE THE GEOGRAPHICAL AREA IN WHICH YOUR AIRTIME RATE APPLIES (OTHER THAN A TEMPORARY DECREASE FOR REPAIRS OR MAINTENANCE), WE'LL DISCLOSE THE CHANGE AT LEAST ONE BILLING CYCLE IN ADVANCE (EITHER THROUGH A NOTICE WITH YOUR BILL, A TEXT MESSAGE TO YOUR DEVICE, OR OTHERWISE), AND YOU MAY TERMINATE THIS AGREEMENT WITHOUT PAYING AN EARLY TERMINATION FEE OR RETURNING OR PAYING FOR ANY PROMOTIONAL ITEMS, PROVIDED YOUR NOTICE OF TERMINATION IS DELIVERED TO US WITHIN THIRTY (30) DAYS AFTER THE FIRST BILL REFLECTING THE CHANGE.

If you lose your eligibility for a particular rate plan, we may change your rate plan to one for which you qualify.

1.4 How Will I Receive My Bill? What Charges Am I Responsible For? How Much Time Do I Have To Dispute My Bill?

You will receive an electronic (paperless) bill at AT&T's online account management site unless you tell us you want a paper bill. You will be given the option to choose electronic billing or paper billing when you purchase service. Each month we will send you an email notice when your electronic bill is available online. This will be sent to your official email address on file with AT&T. You are required to keep your email address current and to notify us immediately of any change in your email address. You always have the option of switching back to a paper bill by changing your billing preferences at AT&T's online account management site. You will not receive a paper bill in the mail unless you expressly request one.

You are responsible for paying all charges for or resulting from Services provided under this Agreement, including any activation fee that may apply to each voice or data line. You will receive monthly bills that are due in full.

IF YOU DISPUTE ANY CHARGES ON YOUR BILL, YOU MUST NOTIFY US IN WRITING AT AT&T BILL DISPUTE, 1025 LENOX PARK, ATLANTA, GA 30319 WITHIN 100 DAYS OF THE DATE OF THE BILL OR YOU'LL HAVE WAIVED YOUR RIGHT TO DISPUTE THE BILL AND TO PARTICIPATE IN ANY LEGAL ACTION RAISING SUCH DISPUTE.

Charges include, without limitation, airtime, roaming, recurring monthly service, activation, administrative, and late payment charges; regulatory cost recovery and other surcharges; optional feature charges; toll, collect call and directory assistance charges; restoral and reactivation charges; any other charges or calls billed to your phone number; and applicable taxes and governmental fees, whether assessed directly upon you or upon AT&T.

To determine your primary place of use ("PPU") and which jurisdiction's taxes and assessments to collect, you're required to provide us with your residential or business street address. If you don't provide us with such address, or if it falls outside our licensed Services area, we may reasonably designate a PPU within the licensed Services area for you. You must live and have a mailing address within AT&T's owned network coverage area.

Auto Bill Pay: If you enroll your account for automatic bill payments ("Auto Bill Pay"), you authorized AT&T to charge your debit/credit card or bank account automatically to pay your monthly statements, as well as any unpaid balances and fees if your AT&T service is disconnected. To cancel your authorization for Auto Bill Pay, you must call 1-800-288-2020. You should also contact your card issuer or financial institution to advise that you have cancelled your enrollment. You will lose any promotional credits associated with your account if you opt out from Auto Bill Pay.

1.5 How Does AT&T Calculate My Bill?

Usage and monthly fees will be billed as specified in your customer service summary or rate plan information online. If the Equipment you order is shipped to you, your Services may be activated before you take delivery of the Equipment so that you can use it promptly upon receipt. Thus, you may be charged for Services while your Equipment is still in transit. If, upon receiving your first bill, you have been charged for Services while your Equipment was in transit, you may contact Customer Care 1-800-331-0500 to request a credit. Except as provided below, monthly Services and certain other charges are billed one month in advance, and there is no proration of such charges if Service is terminated on other than the last day of your billing cycle. Monthly Service and certain other charges are billed in arrears if you're a former customer of AT&T Wireless and maintain uninterrupted Service on select AT&T rate plans, however, if you elect to receive your bills for your Services combined with your wireline phone bill (where available) you will be billed in advance as provided above. You agree to pay for all services used with your Device.

AIRTIME AND OTHER MEASURED USAGE ("CHARGEABLE TIME") IS BILLED IN FULL-MINUTE INCREMENTS, AND ACTUAL AIRTIME AND USAGE ARE ROUNDED UP TO THE NEXT FULL-MINUTE INCREMENT AT THE END OF EACH CALL FOR BILLING PURPOSES. AT&T CHARGES A FULL MINUTE OF AIRTIME USAGE FOR EVERY FRACTION OF THE LAST MINUTE OF AIRTIME USED ON EACH WIRELESS CALL. UNLESS OTHERWISE PROVIDED IN YOUR PLAN, MINUTES WILL BE DEPLETED ACCORDING TO USAGE IN THE FOLLOWING ORDER: NIGHT AND WEEKEND MINUTES, MOBILE TO MOBILE MINUTES, ANYTIME MINUTES AND ROLLOVER, EXCEPT THAT MINUTES THAT ARE PART OF BOTH A LIMITED PACKAGE AND AN UNLIMITED PACKAGE WILL NOT BE DEPLETED FROM THE LIMITED PACKAGE. Chargeable Time begins for outgoing calls when you press SEND (or similar key) and for incoming calls when a signal connection from the caller is established with our facilities. Chargeable Time ends after you press END (or similar key), but not until your wireless telephone's signal of call disconnect is received by our facilities and the call disconnect signal has been confirmed.

All outgoing calls for which we receive answer supervision or which have at least 30 seconds of Chargeable Time, including ring time, shall incur a minimum of one minute airtime charge. Answer supervision is generally received when a call is answered; however, answer supervision may also be generated by voicemail systems, private branch exchanges, and interexchange switching equipment. Chargeable Time may include time for us to recognize that only one party has disconnected from the call, time to clear the channels in use, and ring time. Chargeable Time may also occur from other uses of our facilities, including by way of example, voicemail deposits and retrievals, and call transfers. Calls that begin in one rate period and end in another rate period may be billed in their entirety at the rates for the period in which the call began.

DATA TRANSPORT OR USAGE IS CALCULATED IN FULL-KILOBYTE INCREMENTS, AND ACTUAL TRANSPORT OR USAGE IS ROUNDED UP TO THE NEXT FULL-KILOBYTE INCREMENT AT THE END OF EACH DATA SESSION FOR BILLING PURPOSES. AT&T CALCULATES A FULL KILOBYTE OF DATA TRANSPORT/USAGE FOR EVERY FRACTION

OF THE LAST KILOBYTE OF DATA TRANSPORT/USAGE USED ON EACH DATA SESSION. TRANSPORT OR USAGE IS BILLED EITHER BY THE KILOBYTE ("KB") OR MEGABYTE ("MB"). IF BILLED BY MB, THE FULL KBs CALCULATED FOR EACH DATA SESSION DURING THE BILLING PERIOD ARE TOTALED AND ROUNDED UP TO NEXT FULL MB INCREMENT TO DETERMINE BILLING. IF BILLED BY KB, THE FULL KBs CALCULATED FOR EACH DATA SESSION DURING THE BILLING PERIOD ARE TOTALED TO DETERMINE BILLING. NETWORK OVERHEAD, SOFTWARE UPDATE REQUESTS, EMAIL NOTIFICATIONS, AND RESEND REQUESTS CAUSED BY NETWORK ERRORS CAN INCREASE MEASURED KILOBYTES. DATA TRANSPORT/USAGE OCCURS WHENEVER YOUR DEVICE IS CONNECTED TO OUR NETWORK AND IS ENGAGED IN ANY DATA TRANSMISSION, AS DISCUSSED IN MORE DETAIL IN SECTION 6.4.

If you select a rate plan that includes a predetermined allotment of Services (for example, a predetermined amount of airtime, megabytes or messages), unless otherwise specifically provided as a part of such rate plan, any unused allotment of Services from one billing cycle will not carry over to any other billing cycle. We may bill you in a format as we determine from time to time. Additional charges may apply for additional copies of your bill, or for detailed information about your usage of Services.

Delayed Billing: Billing of usage for calls, messages, data or other Services (such as usage when roaming on other carriers' networks, including internationally) may occasionally be delayed. Such usage charges may appear in a later billing cycle, will be deducted from Anytime monthly minutes or other Services allotments for the month when the usage is actually billed, and may result in additional charges for that month. Those minutes will be applied against your Anytime monthly minutes in the month in which the calls appear on your bill. You also remain responsible for paying your monthly Service fee if your Service is suspended for nonpayment. We may require payment by money order, cashier's check, or a similarly secure form of payment at our discretion.

1.6 Are Advance Payments And/Or Deposits Required?

We may require you to make deposits or advance payments for Services, which we may offset against any unpaid balance on your account. Interest won't be paid on advance payments or deposits unless required by law. We may require additional advance payments or deposits if we determine that the initial payment was inadequate. Based on your creditworthiness as we determine it, we may establish a credit limit and restrict Services or features. If your account balance goes beyond the limit we set for you, we may immediately interrupt or suspend Services until your balance is brought below the limit. Any charges you incur in excess of your limit become immediately due. If you have more than one account with us, you must keep all accounts in good standing to maintain Services. If one account is past due or over its limit, all accounts in your name are subject to interruption or termination and all other available collection remedies.

1.7 What if I fail to pay my AT&T Bill when it is due?

You agree that for each bill not paid in full by the due date, AT&T may charge and you will pay a

late payment fee of \$5.75. Restrictive endorsements are void.

You expressly authorize, and specifically consent to allowing, AT&T and/or its outside collection agencies, outside counsel, or other agents to contact you in connection with any and all matters relating to unpaid past due charges billed by AT&T to you. You agree that, for attempts to collect unpaid past due charges, such contact may be made to any mailing address, telephone number, cellular phone number, e-mail address, or any other electronic address that you have provided, or may in the future provide, to AT&T. You agree and acknowledge that any e-mail address or any other electronic address that you provide to AT&T is your private address and is not accessible to unauthorized third parties. For attempts to collect unpaid charges, you agree that in addition to individual persons attempting to communicate directly with you, any type of contact described above may be made using, among other methods, pre-recorded or artificial voice messages delivered by an automatic telephone dialing system, pre-set e-mail messages delivered by an automatic e-mailing system, or any other pre-set electronic messages delivered by any other automatic electronic messaging system.

1.8 What Happens If My Check Bounces?

We'll charge you up to \$30 (depending on applicable law) for any check or other instrument (including credit card charge backs) returned unpaid for any reason.

1.9 Are There Business or Government Benefits?

You may receive or be eligible for certain discounts, credits, promotions, and other benefits ("Benefits") through a business or government customer's agreement with us ("Business Agreement"). All such Benefits are provided to you solely as a result of the corresponding Business Agreement, and may be modified or terminated without notice. You may also be eligible for certain additional rate plans and/or other Services. Please see <http://www.att.com/iru-additional-terms> for such Services and the associated additional terms, which are hereby incorporated by reference.

If a business or government entity pays your charges or is otherwise liable for the charges, you authorize us to share your account information with it or its authorized agents. If you use Service (s) and/or receive certain Benefits tied to a Business Agreement with us, but you're liable for your own charges, then you authorize us to share enough account information with it or its authorized agents to verify your continuing eligibility for those Services or Benefits.

You may receive Benefits because of your agreement to have the charges for your Services, billed ("Joint Billing") by a wireline company affiliated with AT&T ("Affiliate") or because you subscribe to certain services provided by an Affiliate. If you cancel Joint Billing or the Affiliate service your rates will be adjusted without notice to a rate plan for which you qualify.

1.10 Who Can Access My Account and for What Purpose?

You may add an Authorized/Approved User to Your account. Doing so authorizes Us to provide the Authorized/Approved User with information about, and access to, Your account.

Authorized/Approved Users include:

- (a) A person authorized by You to act on Your behalf with respect to Your account when the person is in a retail store;
- (b) A person who calls into customer service and provides sufficient account information; and
- (c) A person who registers for secondary access to Your account in AT&T's online account management system, provides sufficient account information, and has access to a device that is billed to Your account.

Authorized/Approved Users can view Your account and payment information, make changes to the plans under Your account, purchase devices including via financing agreements, add new lines of service, and perform other account functions. You are responsible for all changes made or actions taken by Authorized/Approved Users.

By taking these actions as Your agent, Authorized/Approved Users authorize Us to perform a credit check on You, share Your credit information between Us and our Affiliates, and obtain a credit report on You from a consumer reporting agency.

You may remove an Authorized/Approved User at any time by contacting Us. The removal will take effect after we have a reasonable opportunity to process the request. If You remove an Authorized/Approved User, we recommend that You reset your account passcode and online credentials.

You consent to the use by us or our authorized agents of regular mail, predictive or autodialing equipment, email, text messaging, facsimile or other reasonable means to contact you to advise you about our Services or other matters we believe may be of interest to you. In any event, we reserve the right to contact you by any means regarding customer service-related notifications, or other such information.

1.11 How will AT&T communicate with me about my Service?

As your wireless carrier, we will need to communicate with you about your Service on occasion. We and our authorized agents may contact you by: bill message, text message, email, phone call, postal mail, in-app notification, push notification, or by other reasonable means, to advise you about your Service or other matters we believe may be of interest to you. **We and our authorized agents may use any one or a combination of these methods of communication to convey important notices (for example, changes to this Agreement, to your Service, legal notices, etc.). You expressly consent on behalf of all the wireless lines on your account to all such methods of communication regarding your Service, whether active or inactive.**

Email and text messages to your AT&T device are two of the primary methods that we use to contact you. The email address you provide at the time of ordering or Service activation is the email address we will use to communicate with you. You can update your email address through myAT&T, using the myAT&T app, or by calling Customer Care at 800.331.0500. **Notices from us to you are considered immediately delivered when we send them to your email address or by text message to your AT&T device.**

Bill messages and inserts are another key way we share information with you. If you have online billing, those notices will be deemed received by you when your online bill is available for viewing. If you get a paper bill, those notices will be deemed received by you three days after we mail the bill to you. **Please do not overlook the important messages section of your bill.**

2.0 HOW DO I RESOLVE DISPUTES WITH AT&T?

2.1 Dispute Resolution By Binding Arbitration

PLEASE READ THIS CAREFULLY. IT AFFECTS YOUR RIGHTS.

Summary:

Most customer concerns can be resolved quickly and to the customer's satisfaction by calling our customer service department at 1-800-331-0500. **In the unlikely event that AT&T's customer service department is unable to resolve a complaint you may have to your satisfaction (or if AT&T has not been able to resolve a dispute it has with you after attempting to do so informally), we each agree to resolve those disputes through binding arbitration or small claims court instead of in courts of general jurisdiction.** Arbitration is more informal than a lawsuit in court. Arbitration uses a neutral arbitrator instead of a judge or jury, allows for more limited discovery than in court, and is subject to very limited review by courts. Arbitrators can award the same damages and relief that a court can award. **Any arbitration under this Agreement will take place on an individual basis; class arbitrations and class actions are not permitted.** For any non-frivolous claim that does not exceed \$75,000, AT&T will pay all costs of the arbitration. Moreover, in arbitration you are entitled to recover attorneys' fees from AT&T to at least the same extent as you would be in court.

In addition, under certain circumstances (as explained below), AT&T will pay you more than the amount of the arbitrator's award and will pay your attorney (if any) twice his or her reasonable attorneys' fees if the arbitrator awards you an amount that is greater than what AT&T has offered you to settle the dispute.

2.2 Arbitration Agreement

1. AT&T and you agree to arbitrate **all disputes and claims** between us. This agreement to arbitrate is intended to be broadly interpreted. It includes, but is not limited to:
 - claims arising out of or relating to any aspect of the relationship between us, whether based in contract, tort, statute, fraud, misrepresentation or any other legal theory;

- claims that arose before this or any prior Agreement (including, but not limited to, claims relating to advertising);
- claims that are currently the subject of purported class action litigation in which you are not a member of a certified class; and
- claims that may arise after the termination of this Agreement.

References to "AT&T," "you," and "us" include our respective subsidiaries, affiliates, agents, employees, predecessors in interest, successors, and assigns, as well as all authorized or unauthorized users or beneficiaries of services or Devices under this or prior Agreements between us. Notwithstanding the foregoing, either party may bring an individual action in small claims court. This arbitration agreement does not preclude you from bringing issues to the attention of federal, state, or local agencies, including, for example, the Federal Communications Commission. Such agencies can, if the law allows, seek relief against us on your behalf. **You agree that, by entering into this Agreement, you and AT&T are each waiving the right to a trial by jury or to participate in a class action.** This Agreement evidences a transaction in interstate commerce, and thus the Federal Arbitration Act governs the interpretation and enforcement of this provision. This arbitration provision shall survive termination of this Agreement.

2. A party who intends to seek arbitration must first send to the other, by certified mail, a written Notice of Dispute ("Notice"). The Notice to AT&T should be addressed to: Office for Dispute Resolution, AT&T, 1025 Lenox Park Blvd., Atlanta, GA 30319 ("Notice Address"). The Notice must (a) describe the nature and basis of the claim or dispute; and (b) set forth the specific relief sought ("Demand"). If AT&T and you do not reach an agreement to resolve the claim within 30 days after the Notice is received, you or AT&T may commence an arbitration proceeding. During the arbitration, the amount of any settlement offer made by AT&T or you shall not be disclosed to the arbitrator until after the arbitrator determines the amount, if any, to which you or AT&T is entitled. You may download or copy a form Notice and a form to initiate arbitration at att.com/arbitration-forms.
3. After AT&T receives notice at the Notice Address that you have commenced arbitration, it will promptly reimburse you for your payment of the filing fee, unless your claim is for greater than \$75,000. (The filing fee currently is \$200 for claims under \$10,000 but is subject to change by the arbitration provider. If you are unable to pay this fee, AT&T will pay it directly upon receiving a written request at the Notice Address.) The arbitration will be governed by the Commercial Arbitration Rules and the Supplementary Procedures for Consumer Related Disputes (collectively, "AAA Rules") of the American Arbitration Association ("AAA"), as modified by this Agreement, and will be administered by the AAA. The AAA Rules are available online at adr.org, by calling the AAA at 1-800-778-7879, or by writing to the Notice Address. (You may obtain information that is designed for non-lawyers about the arbitration process at att.com/arbitration-information.) The arbitrator is bound by the terms of this Agreement. All issues are for the arbitrator to decide, except that issues relating to the scope and enforceability of the arbitration provision are for the court to decide. Unless AT&T and you agree otherwise, any arbitration hearings will take place in the county (or parish) of your billing address. If your claim is for \$10,000 or less, we agree that you may choose whether the arbitration will be conducted solely on the basis of documents submitted to the arbitrator,

through a telephonic hearing, or by an in-person hearing as established by the AAA Rules. If your claim exceeds \$10,000, the right to a hearing will be determined by the AAA Rules. Regardless of the manner in which the arbitration is conducted, the arbitrator shall issue a reasoned written decision sufficient to explain the essential findings and conclusions on which the award is based. Except as otherwise provided for herein, AT&T will pay all AAA filing, administration, and arbitrator fees for any arbitration initiated in accordance with the notice requirements above. If, however, the arbitrator finds that either the substance of your claim or the relief sought in the Demand is frivolous or brought for an improper purpose (as measured by the standards set forth in Federal Rule of Civil Procedure 11(b)), then the payment of all such fees will be governed by the AAA Rules. In such case, you agree to reimburse AT&T for all monies previously disbursed by it that are otherwise your obligation to pay under the AAA Rules. In addition, if you initiate an arbitration in which you seek more than \$75,000 in damages, the payment of these fees will be governed by the AAA rules.

4. If, after finding in your favor in any respect on the merits of your claim, the arbitrator issues you an award that is greater than the value of AT&T's last written settlement offer made before an arbitrator was selected, then AT&T will:
 - pay you the amount of the award or \$10,000 ("the alternative payment"), whichever is greater; and
 - pay your attorney, if any, twice the amount of attorneys' fees, and reimburse any expenses (including expert witness fees and costs) that your attorney reasonably accrues for investigating, preparing, and pursuing your claim in arbitration ("the attorney premium").

If AT&T did not make a written offer to settle the dispute before an arbitrator was selected, you and your attorney will be entitled to receive the alternative payment and the attorney premium, respectively, if the arbitrator awards you any relief on the merits. The arbitrator may make rulings and resolve disputes as to the payment and reimbursement of fees, expenses, and the alternative payment and the attorney premium at any time during the proceeding and upon request from either party made within 14 days of the arbitrator's ruling on the merits.

5. The right to attorneys' fees and expenses discussed in paragraph (4) supplements any right to attorneys' fees and expenses you may have under applicable law. Thus, if you would be entitled to a larger amount under the applicable law, this provision does not preclude the arbitrator from awarding you that amount. However, you may not recover duplicative awards of attorneys' fees or costs. Although under some laws AT&T may have a right to an award of attorneys' fees and expenses if it prevails in an arbitration, AT&T agrees that it will not seek such an award.
6. The arbitrator may award declaratory or injunctive relief only in favor of the individual party seeking relief and only to the extent necessary to provide relief warranted by that party's individual claim. **YOU AND AT&T AGREE THAT EACH MAY BRING CLAIMS AGAINST THE OTHER ONLY IN YOUR OR ITS INDIVIDUAL CAPACITY, AND NOT AS A PLAINTIFF OR CLASS MEMBER IN ANY PURPORTED CLASS OR REPRESENTATIVE PROCEEDING.** Further, unless both you and AT&T agree otherwise, the arbitrator may not consolidate more than one person's claims, and may not otherwise preside over any form of

a representative or class proceeding. If this specific provision is found to be unenforceable, then the entirety of this arbitration provision shall be null and void.

7. Notwithstanding any provision in this Agreement to the contrary, we agree that if AT&T makes any future change to this arbitration provision (other than a change to the Notice Address) during your Service Commitment, you may reject any such change by sending us written notice within 30 days of the change to the Arbitration Notice Address provided above. By rejecting any future change, you are agreeing that you will arbitrate any dispute between us in accordance with the language of this provision.

2.3 Puerto Rico Customers

For Puerto Rico customers, references to "small claims court" in sections 2.1 and 2.2 should be understood to mean the Puerto Rico Telecommunications Regulatory Board.

3.0 TERMS RELATING TO YOUR DEVICE AND CONTENT

3.1 Your Device

Your Device must be compatible with, and not interfere with, our Services and must comply with all applicable laws, rules, and regulations. We may periodically program your Device remotely with system settings for roaming service, to direct your Device to use network services most appropriate for your typical usage, and other features that cannot be changed manually. Some device manufacturers will no longer pre-load certain applications into the device memory. As a result, AT&T may remotely pre-load certain applications to your device at activation and periodically update those applications. You can delete any application that AT&T remotely pre-loads on your device.

You agree that you won't make any modifications to your Equipment or its programming to enable the Equipment to operate on any other system. AT&T may, at its sole and absolute discretion, modify the programming to enable the operation of the Equipment on other systems.

If you bought a Device from AT&T, it may have been programmed with a SIM lock which will prevent it from operating with other compatible wireless telephone carriers' services. If you wish to use this Device with the service of another wireless telephone carrier, you must enter a numeric Unlock Code to unlock the phone. AT&T will provide the Unlock Code upon request, provided that you meet certain criteria including, but not limited to the following: (a) you have paid for your Device in full; (b) your account has been active for at least sixty days and is in good standing (i.e. it has no past due amount or unpaid balance owed AT&T); (c) you have fulfilled your Service Commitment by expiration of any contractual term, upgrading to a new Device under AT&T's standard or early upgrade policies, or payment of any applicable ETF; (d) your Device has not been reported lost or stolen; and (e) AT&T has the Unlock Code or can reasonably obtain it from the manufacturer. AT&T will unlock a maximum of five phones per account, per year. For Devices sold with a Prepaid Plan, AT&T will provide you with the Unlock Code upon request if you provide a detailed receipt or other proof of purchase of the phone and

AT&T has the Unlock Code or can reasonably obtain it from the manufacturer. For further details on eligibility requirements and for assistance on obtaining the Unlock Code for your handset, please call 1-800-331-0500 or visit an AT&T company store.

You are solely responsible for complying with U.S. Export Control laws and regulations and the import laws and regulations of foreign countries when traveling internationally with your Device.

3.2 Where and How Does AT&T Service Work?

AT&T does not guarantee availability of wireless network. Services may be subject to certain Device and compatibility/limitations including memory, storage, network availability, coverage, accessibility and data conversion limitations. Services (including without limitation, eligibility requirements, plans, pricing, features and/or service areas) are subject to change without notice.

When outside AT&T's coverage area, access will be limited to information and applications previously downloaded to or resident on your device. Coverage areas vary between AT&T network technologies. See coverage map(s), available at store or from your sales representative, for details or the coverage map at www.att.com/coverageviewer.

Actual network speeds depend upon device characteristics, network, network availability and coverage levels, tasks, file characteristics, applications and other factors. Performance may be impacted by transmission limitations, terrain, in-building/in-vehicle use and capacity constraints.

3.3 What Information, Content, And Applications Are Provided By Third Parties?

Certain information, applications, or other content is provided by independently owned and operated content providers or service providers who are subject to change at any time without notice.

AT&T IS NOT A PUBLISHER OF THIRD-PARTY INFORMATION, APPLICATIONS, OR OTHER CONTENT AND IS NOT RESPONSIBLE FOR ANY OPINIONS, ADVICE, STATEMENTS, OR OTHER INFORMATION, SERVICES OR GOODS PROVIDED BY THIRD PARTIES.

Third-party content or service providers may impose additional charges. Policies regarding intellectual property, privacy and other policies or terms of use may differ among AT&T's content or service providers and you are bound by such policies or terms when you visit their respective sites or use their services. It is your responsibility to read the rules or service agreements of each content provider or service provider.

Any information you involuntarily or voluntarily provide to third parties is governed by their policies or terms. The accuracy, appropriateness, content, completeness, timeliness, usefulness, security, safety, merchantability, fitness for a particular purpose, transmission or correct sequencing of any application, information or downloaded data is not guaranteed or warranted by AT&T or any content providers or other third party. Delays or omissions may occur. Neither AT&T nor its content providers, service providers or other third parties shall be liable to you for

any loss or injury arising out of or caused, in whole or in part, by your use of any information, application or content, or any information, application, or other content acquired through the Service.

You acknowledge that every business or personal decision, to some degree or another, represents an assumption of risk, and that neither AT&T nor its content and service providers or suppliers, in providing information, applications or other content or services, or access to information, applications, or other content underwrites, can underwrite, or assumes your risk in any manner whatsoever.

3.4 How Can I Get Mobile Content?

You understand that Devices can be used to acquire or purchase goods, content, and services (including subscription plans) like ring tones, graphics, games, applications and news alerts from AT&T or other companies ("Content"). You understand that you are responsible for all authorized charges associated with such Content from any Device assigned to your account, that these charges will appear on your bill (including charges on behalf of other companies), and that such purchases can be restricted by using parental controls available from an AT&T salesperson, or by calling AT&T. Any person using any Device assigned to your account to order Content on your account may be deemed to have corresponding authority to consent to the use or disclosure of your account information, including customer proprietary network information (CPNI), to facilitate the processing or provisioning of and/or billing for such Content. CPNI is information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service, and you have the right, and AT&T has the duty under federal law, to protect the confidentiality of CPNI. You have the right to withhold authorization of this disclosure and use of your CPNI without affecting the provision of any service(s) to which you currently subscribe from AT&T.

You are responsible for reviewing your monthly bills to ensure that all charges for Content are accurate.

Additionally, you have full-time access to your Content purchase transaction history on our website. You may contest and seek refunds for unauthorized purchases and purchases with which you are not satisfied. AT&T reserves the right to restrict Content purchases or terminate the account of anyone who seeks refunds on improper grounds or otherwise abuses this Service.

Actual Content may vary based on the Device capabilities. Content may be delivered in multiple messages. Content charges are incurred at the stated one-time download rate or subscription rate, plus a per kilobyte or per megabyte default pay per use charge for the Content transport when delivered, unless you have a data plan and such charges appear separately on your bill. You will be charged each time you download Content. Data Service charges apply.

3.5 Am I Responsible If Someone Makes A Purchase With My Device?

Except as otherwise provided in this Agreement, if your Device is used by others to make Content purchases, you are responsible for all such purchases. If this occurs, you are giving those other users your authority to:

1. make Content purchases from those Devices, and to incur charges for those Content purchases that will appear on your bill;
2. give consent required for that Content, including the consent to use that user's location information to deliver customized information to that user's Device; or
3. make any representation required for that content, including a representation of the user's age, if requested.

Usage by others can be restricted by use of parental controls or similar features. Visit att.com/smartlimits to learn more.

3.6 Does AT&T Collect Location-Based Network Performance Information From My Device? Can I Use Location-Based Services With My Device?

AT&T collects information about the approximate location of your Device in relation to our cell towers and the Global Positioning System (GPS). We use that information, as well as other usage and performance information also obtained from our network and your Device, to provide you with wireless voice and data services, and to maintain and improve our network and the quality of your wireless experience. We may also use location information to create aggregate data from which your personally identifiable information has been removed or obscured. Such aggregate data may be used for a variety of purposes such as scientific and marketing research and services such as vehicle traffic volume monitoring. It is your responsibility to notify users on your account that we may collect and use location information from Devices.

Your Device is also capable of using optional Content at your request or the request of a user on your account, offered by AT&T or third parties that make use of a Device's location information ("Location-Based Services"). Please review the terms and conditions and the associated privacy policy for each Location-Based Service to learn how the location information will be used and protected. For more information on Location-Based Services, please visit att.com/privacy.

Our directory assistance service (411) may use the location of a Device to deliver relevant customized 411 information based upon the user's request for a listing or other 411 service. By using this directory assistance service, the user is consenting to our use of that user's location information for such purpose. This location information may be disclosed to a third party to perform the directory assistance service and for no other purpose. Such location information will be retained only as long as is necessary to provide the relevant customized 411 information and will be discarded after such use. Please see our privacy policy at att.com/privacy for additional details.

3.7 What If My Device Is Lost Or Stolen?

If your wireless Device is lost or stolen, you must contact us immediately to report the Device lost or stolen. You're not liable for charges you did not authorize, but the fact that a call was placed from your Device is evidence that the call was authorized. Once you report to us that the Device is lost or stolen, you will not be responsible for subsequent charges incurred by that Device.

You can report your Device as lost or stolen and suspend Services without a charge by contacting us at the phone number listed on your bill or at wireless.att.com. If there are charges on your bill for calls made after the Device was lost or stolen, but before you reported it to us, notify us of the disputed charges and we will investigate. You may submit documents, statements and other information to show any charges were not authorized. You may be asked to provide information and you may submit information to support your claim. We will advise you of the result of our investigation within 30 days. While your phone is suspended you will remain responsible for complying with all other obligations under this Agreement, including, but not limited to, your monthly fee. We both have a duty to act in good faith in a reasonable and responsible manner including in connection with the loss or theft of your Device. (California Customers see Section 11.1 "California: What if there are Unauthorized Charges Billed to My Device?" below.)

4.0 TERMS RELATING TO THE USE AND LIMITATIONS OF SERVICE

4.1 What Are The Limitations On Service And Liability?

Unless prohibited by law, the following limitations of liability apply. Service may be interrupted, delayed, or otherwise limited for a variety of reasons, including environmental conditions, unavailability of radio frequency channels, system capacity, priority access by National Security and Emergency Preparedness personnel in the event of a disaster or emergency, coordination with other systems, equipment modifications and repairs, and problems with the facilities of interconnecting carriers. We may block access to certain categories of numbers (e.g., 976, 900, and international destinations) at our sole discretion.

Additional hardware, software, subscription, credit or debit card, Internet access from your compatible PC and/or special network connection may be required and you are solely responsible for arranging for or obtaining all such requirements. Some solutions may require third party products and/or services, which are subject to any applicable third party terms and conditions and may require separate purchase from and/or agreement with the third party provider. AT&T is not responsible for any consequential damages caused in any way by the preceding hardware, software or other items/requirements for which you are responsible.

Not all plans or Services are available for purchase or use in all sales channels, in all areas or with all devices. AT&T is not responsible for loss or disclosure of any sensitive information you transmit. AT&T's wireless services are not equivalent to wireline Internet. AT&T is not responsible for nonproprietary services or their effects on devices.

We may, but do not have the obligation to, refuse to transmit any information through the Services and may screen and delete information prior to delivery of that information to you. There are gaps in service within the Services areas shown on coverage maps, which, by their nature, are only approximations of actual coverage.

WE DO NOT GUARANTEE YOU UNINTERRUPTED SERVICE OR COVERAGE. WE CANNOT ASSURE YOU THAT IF YOU PLACE A 911 CALL YOU WILL BE FOUND. AIRTIME AND OTHER SERVICE CHARGES APPLY TO ALL CALLS, INCLUDING INVOLUNTARILY TERMINATED CALLS. AT&T MAKES NO WARRANTY, EXPRESS OR IMPLIED, OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, SUITABILITY, ACCURACY, SECURITY, OR PERFORMANCE REGARDING ANY SERVICES, SOFTWARE OR GOODS, AND IN NO EVENT SHALL AT&T BE LIABLE, WHETHER OR NOT DUE TO ITS OWN NEGLIGENCE, for any:

- a. act or omission of a third party;
- b. mistakes, omissions, interruptions, errors, failures to transmit, delays, or defects in the Services or Software provided by or through us;
- c. damage or injury caused by the use of Services, Software, or Device, including use in a vehicle;
- d. claims against you by third parties;
- e. damage or injury caused by a suspension or termination of Services or Software by AT&T; or
- f. damage or injury caused by failure or delay in connecting a call to 911 or any other emergency service.

Notwithstanding the foregoing, if your Service is interrupted for 24 or more continuous hours by a cause within our control, we will issue you, upon request, a credit equal to a pro-rata adjustment of the monthly Service fee for the time period your Service was unavailable, not to exceed the monthly Service fee. Our liability to you for Service failures is limited solely to the credit set forth above.

Unless prohibited by law, AT&T isn't liable for any indirect, special, punitive, incidental or consequential losses or damages you or any third party may suffer by use of, or inability to use, Services, Software, or Devices provided by or through AT&T, including loss of business or goodwill, revenue or profits, or claims of personal injuries.

To the full extent allowed by law, you hereby release, indemnify, and hold AT&T and its officers, directors, employees and agents harmless from and against any and all claims of any person or entity for damages of any nature arising in any way from or relating to, directly or indirectly, service provided by AT&T or any person's use thereof (including, but not limited to, vehicular damage and personal injury), INCLUDING CLAIMS ARISING IN WHOLE OR IN PART FROM THE ALLEGED NEGLIGENCE OF AT&T, or any violation by you of this Agreement. This

obligation shall survive termination of your Service with AT&T. AT&T is not liable to you for changes in operation, equipment, or technology that cause your Device or Software to be rendered obsolete or require modification.

SOME STATES, INCLUDING THE STATE OF KANSAS, DON'T ALLOW DISCLAIMERS OF IMPLIED WARRANTIES OR LIMITS ON REMEDIES FOR BREACH. THEREFORE, THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS AGREEMENT GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

4.2 How Can I Use My AT&T Service?

All use of AT&T's wireless network and Services is governed by AT&T's Acceptable Use Policy, which can be found at att.com/AcceptableUsePolicy, as determined solely by AT&T. AT&T can revise its Acceptable Use Policy at any time without notice by updating this posting.

4.3 Who Is Responsible For Security?

AT&T DOES NOT GUARANTEE SECURITY. Data encryption is available with some, but not all, Services sold by AT&T. If you use your Device to access company email or information, it is your responsibility to ensure your use complies with your company's internal IT and security procedures.

4.4 How Can I Use the Software?

The software, interfaces, documentation, data, and content provided for your Equipment as may be updated, downloaded, or replaced by feature enhancements, software updates, system restore software or data generated or provided subsequently by AT&T (hereinafter "Software") is licensed, not sold, to you by AT&T and/or its licensors/suppliers for use only on your Equipment. Your use of the Software shall comply with its intended purposes as determined by us, all applicable laws, and AT&T's Acceptable Use Policy at att.com/AcceptableUsePolicy.

You are not permitted to use the Software in any manner not authorized by this License. You may not (and you agree not to enable others to) copy, decompile, reverse engineer, disassemble, reproduce, attempt to derive the source code of, decrypt, modify, defeat protective mechanisms, combine with other software, or create derivative works of the Software or any portion thereof. You may not rent, lease, lend, sell, redistribute, transfer or sublicense the Software or any portion thereof. You agree the Software contains proprietary content and information owned by AT&T and/or its licensors/suppliers.

AT&T and its licensors/suppliers reserve the right to change, suspend, terminate, remove, impose limits on the use or access to, or disable access to, the Software at any time without notice and will have no liability for doing so. You acknowledge AT&T's Software licensors/suppliers are intended third party beneficiaries of this license, including the indemnification, limitation of liability, disclaimer of warranty provisions found in this Agreement.

4.5 How Can I Use Another Carrier's Network (Off-Net Usage)?

4.5.1 Voice

If your use of minutes (including unlimited Services) on other carrier networks ("off-net voice usage") during any two consecutive months exceed your off-net voice usage allowance, AT&T may, at its option, terminate your Services, deny your continued use of other carriers' coverage or change your plan to one imposing usage charges for off-net voice usage. Your off-net voice usage allowance is equal to the lesser of 750 minutes or 40% of the Anytime Minutes included with your plan.

4.5.2 Data

If you use Data Services on other carriers' wireless networks ("off-net data usage") your data usage may be reduced to 2G speeds. In addition, if your off-net data usage during any month exceeds your off-net data usage allowance, AT&T may at its option terminate your access to Data Services, deny your continued use of other carriers' coverage, further reduce your off-net data usage speed, or change your plan to one imposing usage charges for off-net data usage. Your off-net data usage allowance is equal to the lesser of 100 megabytes or 20% of the kilobytes included with your plan. You may be required to use a Device programmed with AT&T's preferred roaming database.

4.5.3 Messaging

If you use messaging services (including unlimited Services) on other carrier networks ("off-net messaging usage") during any two consecutive months exceed your off-net messaging usage allowance, AT&T may, at its option, terminate your messaging service, deny your continued use of other carriers' coverage or change your plan to one imposing usage charges for off-net messaging usage. Your off-net messaging usage allowance is equal to the lesser of 3,000 messages or 50% of the messages included with your plan.

4.5.4 Notice

If you exceed your allowances stated above and AT&T determines to suspend or terminate your access, deny your usage of other carrier's coverage, or change your plan to a different plan, AT&T will provide notice and you may terminate this Agreement.

4.6 How Do I Get Service Outside AT&T's Wireless Network (Roaming)?

Services originated or received while outside your plan's included coverage area are subject to roaming charges. Domestic roaming charges for wireless data or voice Services may be charged with some plans when outside AT&T's wireless network. International roaming rates apply for any voice, messaging or data usage incurred outside the U.S., Puerto Rico and U.S. Virgin Islands. Use of Services when roaming is dependent upon roaming carrier's support of applicable network technology and functionality. Display on your device may not indicate whether you will incur roaming charges. Check with roaming carriers individually for support and coverage details.

4.6.1 International Services

Certain eligibility restrictions apply which may be based on service tenure, payment history and/or credit. Rates are subject to change. For countries, rates and additional details, see att.com/global.

4.6.1.1 International Long Distance:

International rates apply for calls made and messages sent from the U.S., Puerto Rico and U.S.V.I. to another country. Calling or messaging to some countries may not be available. Calls to wireless numbers and numbers for special services, such as Premium Rated Services, may cost more than calls to wireline numbers. If a customer calls an overseas wireline number and the call is forwarded to a wireless number, the customer will be charged for a call terminated to a wireless number. International Long Distance calling rates are charged per minute and apply throughout the same footprint in which the customer's airtime package minutes apply.

4.6.1.2 International Long Distance Text, Picture & Video Messaging:

Additional charges apply for premium messages and content. Messages over 300 KBs are billed an additional 50¢/message. For a complete list of countries, please visit att.com/text2world.

4.6.1.3 International Roaming:

Compatible Device required. Your plan may include the capability to make and receive calls and texts and use data while roaming internationally. AT&T, in its sole discretion, may block your ability to use your Device while roaming internationally until eligibility criteria are met. International roaming rates, which vary by country, apply for all calls placed or received while outside the United States, Puerto Rico and U.S.V.I. Please consult att.com/global or call 611 from your mobile device or 800-331-0500 for a list of currently available countries and carriers. All countries may not be available for roaming. All carriers within available countries may not be available on certain plans or packages. Availability, quality of coverage and services while roaming are not guaranteed. When roaming internationally, you will be charged international roaming airtime rates including when incoming calls are routed to voicemail, even if no message is left. Substantial charges may be incurred if Device is taken out of the U.S. even if no services are intentionally used. Billing for international roaming usage may be delayed up to three billing cycles due to reporting between carriers. Taxes are additional. If you want to block the ability to make and receive calls or use data functions while roaming internationally, you may request that by calling 1-314-925-6925 (at no charge from your wireless phone). For AT&T Canada and Mexico Travel Minutes, package and overage rates apply only in Canada or Mexico, and if you remove the package before your monthly bill cycle ends, the included monthly minutes allotment will be reduced proportionately.

4.6.1.4 International Data:

International data rates apply to all data usage outside the U.S., Puerto Rico and U.S.V.I., including accessing cloud-based services to upload/download/stream content.

International data roaming may be reduced to 2G speeds. Many Devices, including iPhone, transmit and receive data messages without user intervention and can generate unexpected charges when powered "on" outside the United States, Puerto Rico and U.S.V.I. AT&T may send "alerts" via SMS or email, to notify you of data usage. These are courtesy alerts. There is no guarantee you will receive them. They are not a guarantee of a particular bill limit. Receipt of Visual Voicemail messages are charged at international data pay-per-use rates unless customer has an international data plan/package, in which case receipt of Visual Voicemail messages decrement Kilobytes included in such plan/package.

4.6.1.5 Data Global Add-Ons and Global Messaging Plans/Packages:

Require that domestic data or messaging capability be in place. Rates apply only for usage within "roam zone" comprised of select carriers. Within the roam zone, overage rate applies if you exceed the MBs allotted for any Data Global Add-On or the messages allotted for any Global Messaging Plan/Package. International roaming pay-per-use rates apply in countries outside the roam zone. See att.com/globalcountries for current roam zone list.

4.6.1.6 Data Connect Global/North America Plans:

Do not include capability to place a voice call and require a 1 year agreement. For specific terms regarding international data plans, see Section 6.10.2 of the Wireless Customer Agreement.

4.6.1.7 Cruise Ship Roaming:

Cruise ship roaming rates apply for calls placed or data used while on the ship.

4.6.1.8 International Miscellaneous

Export Restrictions: You are solely responsible for complying with U.S. Export Control laws and regulations, and the import laws and regulations of foreign countries when traveling internationally with your Device.

5.0 WHAT VOICE SERVICES DOES AT&T OFFER?

5.1 What Are The General Terms That Apply To All AT&T Voice Rate Plans?

You may obtain usage information by calling customer service or using one of our automated systems. **Pricing/Taxes/No Proration:** Prices do not include taxes, directory assistance, roaming, Universal Service Fees, and other surcharges. Final month's charges are not prorated.

Activation Fees: Activation Fee may apply for each new line. **Nights and Weekends:** Nights

are 9:00 p.m. to 6:00 a.m. Weekends are 9:00 p.m. Friday to 6:00 a.m. Monday (based on time of day at the cell site or switch providing your Service). Included long distance calls can be made from the 50 United States, Puerto Rico and U.S. Virgin Islands to the 50 United States, Puerto Rico, U.S. Virgin Islands, Guam and Northern Mariana Islands. Roaming charges do not apply when roaming within the Services area of land-based networks of the 50 United States, Puerto Rico and U.S. Virgin Islands. Additional charges apply to Services used outside the land borders of the U.S., Puerto Rico and U.S. Virgin Islands.

5.2 Voicemail

Unless you subscribe to an Unlimited Voice Plan or are an upstate New York customer subscribing to Enhanced Voicemail, airtime charges apply to calls to your voicemail service, including calls where the caller does not leave a message, because the call has been completed, calls to listen to, send, reply to, or forward messages, or to perform other activities with your voicemail service, including calls forwarded from other phones to your voicemail service. You are solely responsible for establishing and maintaining security passwords to protect against unauthorized use of your voicemail service. For information as to the number of voicemail messages you can store, when voicemail messages will be deleted, and other voicemail features, see att.com/wirelessvoicemail. We reserve the right to change the number of voicemails you can store, the length you can store voicemail messages, when we delete voicemail messages, and other voicemail features without notice. We may deactivate your voicemail service if you do not initialize it within a reasonable period after activation. We will reactivate the service upon your request. See att.com/global for information about using voicemail internationally.

5.3 Voicemail-To-Text (VMTT)

AT&T is not responsible, nor liable for: 1) errors in the conversion of or its inability to transcribe voicemail messages to text/email; 2) lost or misdirected messages; or, 3) content that is unlawful, harmful, threatening, abusive, obscene, tortious, or otherwise objectionable.

We do not filter, edit or control voice, text, or email messages, or guarantee the security of messages. We can interrupt, restrict or terminate VMTT without notice, if your use of VMTT adversely impacts AT&T's network, for example that could occur from abnormal calling patterns or an unusually large number of repeated calls and messages; or if your use is otherwise abusive, fraudulent, or does not comply with the law.

You are solely responsible for and will comply with all applicable laws as to the content of any text messages or emails you receive from VMTT that you forward or include in a reply to any other person. You authorize AT&T or a third party working on AT&T's behalf to listen to, and transcribe all or part of a voicemail message and to convert such voicemail message into text/email, and to use voicemail messages and transcriptions to enhance, train and improve AT&T's speech recognition and transcription services, software and equipment.

Charges for VMTT include the conversion of the voicemail message and the text message sent to your wireless device. Additional charges, however, may apply to receiving email on your wireless device from VMTT, as well as, replying to or forwarding VMTT messages via SMS (text) or email, depending on your plan.

SMS (text messaging) blocking is incompatible with VMTT. (If you do not have a texting plan on your handset, we add a texting pay per use feature when you add VMTT with text delivery.) If you are traveling outside the U.S. coverage area, you will incur international data charges for emails received from VMTT, as well as, charges for emails you respond to or forward from VMTT, unless you have an international data plan and the usage falls within the plan's usage limits.

Transcription times cannot be guaranteed. Customers purchasing email delivery are responsible for providing a correct email address and updating the email address when changes to the email account are made.

If you choose SMS (text) delivery, VMTT only converts the first 480 characters of a voicemail message into text and you will receive up to three text messages of a transcribed message. The transcription, therefore, may not include the entire voicemail message with SMS delivery. Adding VMTT will create a new voicemail box and all messages and greetings will be deleted from your current voicemail box.

5.4 Unlimited Voice Services

Unlimited voice Services are provided primarily for reasonably uninterrupted live dialog between two individuals. If your use of unlimited voice Services for conference calling or call forwarding exceeds 750 minutes per month, AT&T may, at its option, terminate your Service or change your plan to one with no unlimited usage components.

AT&T may, in its sole discretion, terminate your Service or change your plan to one with no unlimited voice usage if it reasonably determines or has a reasonable basis to believe that you are engaged in any of the following prohibited activities: (1) maintaining an open line of communication to provide dispatch or monitoring services; (2) accessing or providing access to multi-party chat line services; (3) using the Service with a SIM box or SIM server network to generate or simulate voice calls; (4) transmitting broadcasts; (5) transmitting pre-recorded materials; (6) telemarketing; (7) initiating autodialed calls; (8) initiating any other calls or connections that are not for the purposes of reasonably uninterrupted live dialog between individuals; (9) using the Service for any fraudulent purpose; (10) reselling or rebilling the Service either alone or as part of any other good or service; or (11) any abusive use of our network or Services.

5.5 Caller ID

Your caller identification information (such as your name and phone number) may be displayed on the Device or bill of the person receiving your call; technical limitations may, in some circumstances, prevent you from blocking the transmission of caller identification information.

Contact customer service for information on blocking the display of your name and number. Caller ID blocking is not available when using Data Services, and your wireless number is transmitted to Internet sites you visit.



5.6 Rollover Minutes

If applicable to your plan, Rollover Minutes accumulate and expire through 12 rolling bill periods. Bill Period 1 (activation) unused Anytime Minutes will not carry over. Bill Period 2 unused Anytime Minutes will begin to carry over. Rollover Minutes accumulated starting with Bill Period 2 will expire each bill period as they reach a 12-bill-period age. Rollover Minutes will also expire immediately upon default or if customer changes to a non-Rollover plan. If you change plans (including the formation of a FamilyTalk plan), or if an existing subscriber joins your existing FamilyTalk plan, any accumulated Rollover Minutes in excess of your new plan or the primary FamilyTalk line's included Anytime Minutes will expire. Rollover Minutes are not redeemable for cash or credit and are not transferable. If you change to non-AT&T Unity plans with Rollover Minutes (including the formation of a FamilyTalk plan) any accumulated Rollover Minutes in excess of your new non-AT&T Unity plan or the primary non-AT&T Unity FamilyTalk line's included Anytime Minutes will expire.

5.7 Mobile To Mobile Minutes

If applicable to your plan, Mobile to Mobile Minutes may be used when directly dialing or receiving calls from any other AT&T wireless phone number from within your calling area. Mobile to Mobile Minutes may not be used for interconnection to other networks. Calls to AT&T voicemail and return calls from voicemail are not included.



5.8 Family Talk Plan

If applicable to your plan, FamilyTalk may require up to a two-year Service Commitment for each line. FamilyTalk plans include only package minutes included with the primary number, and minutes are shared by the additional lines. The rate shown for additional minutes applies to all minutes in excess of the Anytime Minutes. FamilyTalk requires two lines. If the rate plan for the primary number is changed to an ineligible plan or the primary number is disconnected, one of the existing additional lines shall become the primary number on the rate plan previously subscribed to by the former primary number; if only one line remains, it shall be converted to the closest single line rate.



5.9 A-List

A-List is available only with select Nation, FamilyTalk and Unity plans. Nation Plan and Individual Subscribers can place/receive calls to/from up to 5 (and FamilyTalk subscribers can place/receive calls to/from up to 10) wireline or wireless telephone numbers without being charged for airtime minutes. All qualifying lines on a FamilyTalk account share the same 10 A-List numbers. Only standard domestic wireline or wireless numbers may be added and A-List is only for domestic calls. Directory assistance, 900 numbers, chat lines, pay per call numbers, customer's own wireless or Voice Mail access numbers, numbers for call routing services and

call forwarding services from multiple phones, and machine to machine numbers are not eligible. Depending on the PBX system, a private telephone system often serving businesses, AT&T may not be able to determine if your selected PBX A-List number is calling/receiving calls from your wireless number and airtime charges could apply. Forwarded calls will be billed based on the originating number, not the call forwarding number, and airtime charges may apply. Only voice calling is eligible. A-List number selections may only be managed online via MyWireless Account. Selected telephone numbers do not become active until 24 hours after added. AT&T reserves the right to block any A-List number and to reduce the amount of telephone numbers that can be used for A-List without notice. A-List is not eligible on Save/Promotional Plans.

5.10 AT&T Viva MexicoSM ("Mexico Plan") & AT&T Nation /FamilyTalk With Canada ("Canada Plan")

Certain eligibility requirements apply. Anytime Minutes and Night and Weekend Minutes between Mexico and your U.S. wireless coverage area if you subscribe to the Mexico Plan, or Canada and your U.S. wireless coverage area if you subscribe to the Canada Plan, will be treated for billing purposes as calls to and from your U.S. wireless coverage area.

Calls made from or received in Mexico and Canada cannot exceed your monthly off-net usage allowance (the lesser of 750 min./mo. or 40% of your Anytime Minutes/mo.) in any two consecutive months. Calls made from or received in Mexico and Canada will not qualify as Mobile to Mobile Minutes. Special rates apply for data usage in Mexico and Canada. International long distance text, instant, picture and video messaging rates apply to messaging from the U.S. to Mexico and Canada and international roaming rates apply when such messages are sent from Mexico and Canada.

International Roaming charges apply when using voice and data Services outside Mexico and your U.S. wireless coverage area if you subscribe to the Mexico Plan, and Canada and your U.S. wireless coverage area, if you subscribe to the Canada Plan. International long distance charges apply when calling to areas outside Mexico and your U.S. wireless coverage area if you subscribe to the Mexico Plan, and Canada and your U.S. wireless coverage area if you subscribe to the Canada Plan.

Anytime Minutes are primarily for live dialog between two people. You may not use your Services other than as intended by AT&T and applicable law. Plans are for individual, non-commercial use only and are not for resale. Unlimited Microcell Calling feature cannot be used on accounts with Viva Mexico and Nation Canada calling plans.

5.11 AT&T UnitySM And AT&T UnitySM-FamilyTalk Plans Requirements

5.11.1 Eligibility Requirements:

AT&T local and wireless combined bill required. For residential customers, qualifying AT&T local plan from AT&T required. For business customers, qualifying AT&T local service plan required. Specific AT&T Services that qualify vary by location; see att.com or call 1-800-288-2020. Certain business accounts are not eligible for Unity plans. Discounts on any other

combined-bill wireless plans will be lost if an AT&T Unity plan is added to your combined bill. If an existing wireless plan is upgraded to an AT&T Unity plan, all discounts and promotions will be lost when subscribing to that plan.

5.11.2 AT&T UnitySM Minutes:

AT&T Unity Calling Minutes may be used when directly dialing or receiving calls from any other eligible AT&T wireline or wireless phone number from within your calling area. Calls to AT&T voicemail and return calls from voicemail not included. AT&T Unity Minutes are not included when checking usage for the current billing period.

5.12 VoiceDial Services

Regular airtime charges apply. Mobile to Mobile Minutes do not apply. Calls to 911, 411, 611, 711 and international dialing cannot be completed with VoiceDial Services. Caller ID cannot be blocked. Caller ID will be delivered on calls, even if you have permanently blocked your name and number. For complete terms and conditions, see att.com/voicedial.

5.13 AT&T Messaging Unlimited with Mobile to Any Mobile Calling Feature

Available only with select Nation, FamilyTalk, and BusinessTalk plans and can be discontinued at anytime. Messaging Unlimited Plan required. Mobile to Any Mobile minutes only apply when you directly dial another U.S. mobile number or directly receive a call from another U.S. mobile phone number from within your calling area in the U.S., Puerto Rico, or U.S.V.I. Mobile to Any Mobile is not available with the AT&T Viva Mexico or AT&T Nation/FamilyTalk with Canada plans. Calls made through Voice Connect, calls to directory assistance, and calls to voicemail and return calls from voicemail are not included. Only numbers included in the wireless number database that AT&T uses will be treated as a call to a mobile number or a call received from a mobile number. So for example, Type 1 numbers belonging to other carriers and not included in the industry wireless LNP database, and numbers for which ports to wireless service have not yet completed, will not be treated as a call to a mobile number or a call received from a mobile number. Also calls made to and calls received from mobile toll-free numbers, mobile chat lines, mobile directory assistance, calling applications, numbers for call routing and call forwarding services, and machine to machine numbers are not included.

6.0 WHAT DATA AND MESSAGING SERVICES DOES AT&T OFFER?

6.1 What Are The General Terms That Apply To All Data And Messaging Plans?

AT&T provides wireless data and messaging Services, including but not limited to, features that may be used with Data Services and wireless content and applications ("Data Services"). The absolute capacity of the wireless data network is limited; consequently, Data Services may only be used for permitted activities. Pricing and data allowances for Data Services are device dependent and based on the capabilities and capacity of each Device.

For Data Services with a monthly megabyte (MB) or gigabyte (GB) data allowance, once you exceed your monthly data allowance you will be automatically charged for overage as specified in the applicable rate plan. All data allowances, including overages, must be used in the billing period in which the allowance is provided. Unused data allowances will not roll over to subsequent billing periods.

AT&T data plans are designed for use with only one of the following distinct Device types: (1) Smartphones, (2) basic and Quick Messaging phones, (3) tablets, (4) LaptopConnect cards, (5) stand-alone Mobile Hotspot devices, and (6) Home Bases. A data plan designated for one type of device may not be used with another type of device. For example, a data plan designated for use with a basic phone or a Smartphone may not be used with a LaptopConnect card, tablet, or stand-alone Mobile Hotspot device, by tethering devices together, by SIM card transfer, or any other means. A data tethering plan, however, may be purchased for an additional fee to enable tethering on a compatible device. An Activation Fee may apply for each data line.

Consumer data plans do not allow access to corporate email, company intranet sites, and other business applications. Access to corporate email, company intranet sites, and/or other business applications requires an applicable Enterprise Data plan. Enterprise Email requires an eligible data plan and Device. Terms may vary depending on selected Enterprise Email solution.

AT&T RESERVES THE RIGHT TO TERMINATE YOUR DATA SERVICES WITH OR WITHOUT CAUSE, INCLUDING WITHOUT LIMITATION, UPON EXPIRATION OR TERMINATION OF YOUR WIRELESS CUSTOMER AGREEMENT.

6.2 What Are The Intended Uses Of AT&T's Wireless Data Service?

AT&T's wireless data network is a shared resource, which AT&T manages for the benefit of all of its customers so that they can enjoy a consistent, high-quality mobile broadband experience and a broad range of mobile Internet services, applications and content. However, certain activities and uses of the network by an individual customer or small group of customers can negatively impact the use and enjoyment of the network by others. Therefore, certain activities and uses of AT&T's wireless data service are permitted and others are prohibited. The terms and conditions of your use of AT&T's wireless data service are set forth below.

Permitted Activities. AT&T's wireless data services are intended to be used for the following permitted activities: (i) web browsing; (ii) email; and (iii) intranet access if permitted by your rate plan (for example, access to corporate intranets, email, and individual productivity applications like customer relationship management, sales force, and field service automation); (d) uploading and downloading applications and content to and from the Internet or third-party application stores, and (e) using applications and content without excessively contributing to network congestion.

You agree to use AT&T's wireless data services only for these permitted activities.

Prohibited Activities: AT&T's wireless data services are not intended to be used in any manner which has any of the following effects and such use is prohibited if it: (a) conflicts with applicable law, (b) hinders other customers' access to the wireless network, (c) compromises network security or capacity, (d) excessively and disproportionately contributes to network congestion, (e) adversely impacts network service levels or legitimate data flows, (f) degrades network performance, (g) causes harm to the network or other customers, (h) is resold either alone or as part of any other good or service, (i) tethers a wireless device to a computing device (such as a computer, Smartphone, eBook or eReader, media player, laptop, or other devices with similar functions) through use of connection kits, applications, devices or accessories (using wired or wireless technology) and you have not subscribed to a specific data plan designed for this purpose, or (j) there is a specific data plan required for a particular use and you have not subscribed to that plan.

The following specific uses of AT&T's wireless data service are prohibited:

- AT&T's wireless data services may not be used in any manner that defeats, obstructs or penetrates, or attempts to defeat, obstruct or penetrate the security measures of AT&T's wireless network or systems, or another entity's network or systems; that accesses, or attempts to access without authority, the accounts of others; or that adversely affects the ability of other people or systems to use either AT&T's wireless services or other parties' Internet-based resources. For example, this includes, but is not limited to, malicious software or "malware" that is designed, intentionally or unintentionally, to infiltrate a network or computer system such as spyware, worms, Trojan horses, rootkits, and/or crimeware; "denial of service" attacks against a network host or individual user; and "spam" or unsolicited commercial or bulk email (or activities that have the effect of facilitating unsolicited commercial email or unsolicited bulk e-mail).
- AT&T's wireless data services may not be used in any manner that has the effect of excessively contributing to network congestion, hindering other customers' access to the network, or degrading network performance by maintaining a sustained and continuous wireless data service connection or active wireless Internet connection. For example, this includes, but is not limited to, server devices or host computer applications such as continuous Web camera posts or broadcasts, automatic data feeds, or automated machine-to-machine connections; "auto-responders," "cancel-bots," or similar automated or manual routines that generate excessive amounts of traffic or that disrupt user groups or email use by others; use of the service as a substitute or backup for private lines or full-time or dedicated data connections; peer-to-peer (P2P) file sharing services; and software or other devices that maintain continuous active Internet connections when a connection would otherwise be idle or any "keep alive" functions, unless they adhere to AT&T data retry requirements (as may be modified from time to time).
- AT&T's wireless data services also may not be used with high bandwidth applications, services and content that are not optimized to work with AT&T's wireless data services and, therefore disproportionately and excessively contribute to network congestion. This includes, but is not limited to, redirecting television signals for viewing on computing devices, web broadcasting, and/or the operation of servers, telemetry devices, or supervisory control and

data acquisition devices, unless they meet AT&T's wireless data services optimization requirements.

You agree not to use AT&T's wireless data services for any of these prohibited activities.

AT&T's Rights to Ensure Compliance. You agree that AT&T has the right to take any and all actions necessary to enforce this Section 6.2 if you use AT&T's wireless data services in any manner that is prohibited, including, but not limited to, the following actions:

- AT&T may modify, without advance notice, the permitted and prohibited activities, and the optimization requirements for your wireless data services;
- AT&T may engage in any reasonable network management practice to enhance customer service, to reduce network congestion, to adapt to advances and changes in technology, and/or to respond to the availability of wireless bandwidth and spectrum;
- AT&T may reduce your data throughput speeds at any time or place if your data usage exceeds an applicable, identified usage threshold during any billing cycle. AT&T will provide you with advance notice of the usage threshold applicable to your data plan, or any changes to the applicable usage threshold either by a bill insert, email, text message or other appropriate means;
- AT&T may use reasonable methods to monitor and collect customer usage information to better optimize the operation of the network. Details concerning the information that AT&T collects about its customers, and how it uses and protects that information are addressed in the AT&T Privacy Policy (see att.com/privacy);
- If you are an AT&T unlimited data plan customer, AT&T may migrate you from the unlimited data plan to a tiered data plan and bill you the appropriate monthly fees. We will provide you with notice of this change at least one billing cycle in advance either by a bill insert, email, text message, or other appropriate means;
- AT&T may interrupt, suspend, cancel or terminate your wireless data services without advance notice.

Unlimited Data Customers. If you are an AT&T unlimited data plan customer, you agree that "unlimited" means you pay a fixed monthly charge for wireless data service regardless of how much data you use. You further agree that "unlimited" does not mean that you can use AT&T's wireless data service in any way that you choose or for any prohibited activities, and that if you use your unlimited data plan in any manner that is prohibited, AT&T can limit, restrict, suspend or terminate your data service or switch you to a tiered data plan.

6.3 What Are The Voice And Data Plan Requirements?

A voice plan is required on all voice-capable Devices, unless specifically noted otherwise in the terms governing your plan.

An eligible tiered pricing data plan is required for certain Devices, including iPhones and other designated Smartphones. Eligible voice and tiered pricing data plans cover voice and data usage in the U.S. and do not cover International voice and data usage and charges. If it is determined that you are using a voice-capable Device without a voice plan, or that you are using an iPhone or designated Smartphone without an eligible voice and tiered data plan, AT&T reserves the right

to switch you to the required plan or plans and bill you the appropriate monthly fees. In the case of the tiered data plan, you will be placed on the data plan which provides you with the greatest monthly data usage allowance. If you determine that you do not require that much data usage in a month, you may request a lower data tier at a lower monthly recurring fee.

6.4 How Does AT&T Calculate My Data Usage/Billing?

DATA TRANSPORT/USAGE OCCURS WHENEVER YOUR DEVICE IS CONNECTED TO OUR NETWORK AND IS ENGAGED IN ANY DATA TRANSMISSION, INCLUDING BUT NOT LIMITED TO: (i) SENDING OR RECEIVING EMAIL, DOCUMENTS, OR OTHER CONTENT, (ii) ACCESSING WEBSITES, OR (iii) DOWNLOADING AND USING APPLICATIONS. SOME APPLICATIONS, CONTENT, PROGRAMS, AND SOFTWARE THAT YOU DOWNLOAD OR THAT COMES PRE-LOADED ON YOUR DEVICE AUTOMATICALLY AND REGULARLY SEND AND RECEIVE DATA TRANSMISSIONS IN ORDER TO FUNCTION PROPERLY, WITHOUT YOU AFFIRMATIVELY INITIATING THE REQUEST AND WITHOUT YOUR KNOWLEDGE. FOR EXAMPLE, APPLICATIONS THAT PROVIDE REAL-TIME INFORMATION AND LOCATION-BASED APPLICATIONS CONNECT TO OUR NETWORK, AND SEND AND RECEIVE UPDATED INFORMATION SO THAT IT IS AVAILABLE TO YOU WHEN YOU WANT TO ACCESS IT. IN ADDITION, ANY ADVERTISEMENTS OR ADVERTISER-RELATED MESSAGES OR DATA DELIVERED TO YOUR DEVICE, EVEN IF DELIVERED TO AN APPLICATION, AS WELL AS ANY MESSAGES OR CONTENT THAT INITIATE IN RESPONSE TO AN ADVERTISEMENT, WILL COUNT TOWARD YOUR DATA USAGE. YOU WILL BE BILLED FOR ALL DATA TRANSPORT AND USAGE WHEN YOUR DEVICE IS CONNECTED TO OUR NETWORK, INCLUDING THAT WHICH YOU AFFIRMATIVELY INITIATE OR THAT WHICH RUNS AUTOMATICALLY IN THE BACKGROUND WITHOUT YOUR KNOWLEDGE, AND WHETHER SUCCESSFUL OR NOT. A DATA SESSION INITIATED ON THE AT&T NETWORK WILL CONTINUE ITS CONNECTION OVER THE AT&T NETWORK UNTIL THE DATA TRANSMISSION IS CONCLUDED, EVEN WHEN YOU CONNECT TO A WI-FI NETWORK DURING THE TRANSMISSION.

Unless designated for International or Canada use, prices and included use apply to access and use on AT&T's wireless network and the wireless networks of other companies with which AT&T has a contractual relationship within the United States and its territories (Puerto Rico and the U.S. Virgin Islands), excluding areas within the Gulf of Mexico.

Usage on networks not owned by AT&T is limited as provided in your data plan. Charges will be based on the location of the site receiving and transmitting service and not the location of the subscriber. Mobile Broadband and 4G access requires a compatible device.

Data Service charges paid in advance for monthly or annual Data Services are nonrefundable. Some Data Services may require an additional monthly subscription fee and/or be subject to additional charges and restrictions. Prices do not include taxes, directory assistance, roaming, universal services fees or other surcharges.

In order to assess your usage during an applicable billing period, you may obtain approximate

usage information by calling customer service or using one of our automated systems.

6.5 Text Messaging And Picture/Video Messaging

If you do not enroll in a monthly recurring plan for messaging, data, or Video Share, you may have access to messaging, data, and video share services and be charged on a pay-per-use basis if you use those services.

Messages are limited to 160 characters per message. Premium text and picture/video messages are charged at their stated rates. Standard rates apply to all incoming messages when in the U.S. Different, non-standard per message charges apply to international messages sent from the U.S.

Text, Picture, and Video messages are charged when sent or received, whether read or unread, solicited or unsolicited. AT&T does not guarantee delivery of messages. Text, Picture, and Video messages, including downloaded content, not delivered within 3 days will be deleted. AT&T reserves the right to change this delivery period as needed without notification.

You are charged for each part of messages that are delivered to you in multiple parts. Picture/Video Messaging, data plan, and Text Messaging may need to be provisioned on an account in order to use Picture/Video Messaging. Some elements of Picture/Video messages may not be accessible, viewable, or heard due to limitations on certain wireless phones, PCs, or e-mail.

AT&T reserves the right to change the Picture/Video message size limit at any time without notification. Picture/Video Messaging pricing is for domestic messages only. When a single message is sent to multiple recipients, the sender is charged for one message for each recipient and each recipient is charged for the message received.

Text message notifications may be sent to non-Picture/Video Messaging subscribers if they subscribe to Text Messaging. You may receive unsolicited messages from third parties as a result of visiting Internet sites, and a per-message charge may apply whether the message is read or unread, solicited or unsolicited.

You agree you will not use our messaging services to send messages that contain advertising or a commercial solicitation to any person or entity without their consent. You will have the burden of proving consent with clear and convincing evidence if a person or entity complains you did not obtain their consent. Consent cannot be evidenced by third party lists you purchased or obtained. You further agree you will not use our messaging service to send messages that: (a) are bulk messages (b) are automatically generated; (c) can disrupt AT&T's network; (d) harass or threaten another person (e) interfere with another customer's use or enjoyment of AT&T's Services; (f) generate significant or serious customer complaints, (g) that falsify or mask the sender/originator of the message; or (h) violate any law or regulation. AT&T reserves the right, but is not obligated, to deny, disconnect, suspend, modify and/or terminate your messaging service or messaging services with any associated account(s), or to deny, disconnect, suspend,

modify and/or terminate the account(s), without notice, as to anyone using messaging services in any manner that is prohibited. Our failure to take any action in the event of a violation shall not be construed as a waiver of the right to enforce such terms, conditions, or policies. Advertising and commercial solicitations do not include messaging that: (a) facilitates, completes, or confirms a commercial transaction where the recipient of such message has previously agreed to enter into with the sender of such message; or (b) provides account information, service or product information, warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient of such message.

6.6 Unlimited Messaging

Unlimited Messaging Plans or plans with unlimited messaging include only AT&T's Short Messaging Service (SMS) and Multimedia Messaging Service (MMS) and not any other messaging services or applications. Messages are intended for direct communication between phones and must originate from your phone. Messages sent to tablets, laptops, or other connected devices are excluded from Unlimited Messaging Plans or plans including unlimited messaging. Messages sent through applications may incur data charges. We may terminate or restrict your messaging Service for tethered messaging, excessive use or misuse.

6.7 Mobile Email

Requires e-mail account with compatible internet service provider and a downloaded or preloaded e-mail application for the wireless device. Access and use of Mobile Email is billed by total volume of data sent and received (in kilobytes) in accordance with your data plan. E-mail attachments cannot be sent, downloaded, read, or forwarded on the mobile device. Only a paper clip icon appears indicating an attachment. You must view attachments from your PC. Upgrades to the application may be required in order to continue to use the Service. Wireless data usage charges will apply for downloading the application and any upgrades.

6.8 Mobile Video

Compatible Phone and eligible data plan required. Service not available outside AT&T's Mobile Broadband and 4G coverage areas. Premium content is charged at stated monthly subscription rates or at stated pay per view rates. Content rotates and is subject to withdrawal. Mobile Video is for individual use, not for resale, commercial purposes or public broadcast. Content can only be displayed on the device screen. No content may be captured, downloaded, forwarded, duplicated, stored, or transmitted. The content owner reserves and owns all content rights. All trademarks, service marks, logos, and copyrights not owned by AT&T are the property of their owners. Some Mobile Video content is intended for mature audiences and may be inappropriate for younger viewers. Parental guidance suggested. Use Parental Controls to restrict access to mature content. Content may be provided by independent providers, and AT&T is not responsible for their content. Providers may collect certain information from your use for tracking and managing content usage.

6.9 AT&T Wi-Fi Services

AT&T Wi-Fi service use with a Wi-Fi capable wireless device is subject to the Terms of Services & Acceptable Use Policy ("Terms") found at att.com/attwifitosaup. Your use represents your agreement to those Terms, incorporated herein by reference. AT&T Wi-Fi Basic service is available at no additional charge to wireless customers with select Wi-Fi capable devices and a qualified data rate plan. Other restrictions may apply.

6.10 DataConnect Plans

6.10.1 What Are the General Terms that Apply to All DataConnect Plans?

A voice plan is not required with DataConnect plans.

We may, at our discretion, suspend your account if we believe your data usage is excessive, unusual or is better suited to another rate plan. If you are on a data plan that does not include a monthly MB/GB allowance and additional data usage rates, you agree that AT&T has the right to impose additional charges if you use more than 5 GB in a month; provided that, prior to the imposition of any additional charges, AT&T shall provide you with notice and you shall have the right to terminate your Data Service.

6.10.2 Data Global Add-On/DataConnect Global Plans/DataConnect North America Plans

Available countries, coverage and participating international carriers included in the "Select International Roam Zone" and "Select Canada/Mexico Roam Zone" vary from our generally available Canada/international wireless data roam zones and may not be as extensive. The Select International Roam Zone is restricted to select international wireless carrier(s). Select Canada/Mexico Roam Zone is restricted to select wireless carrier(s) and coverage areas within Canada and Mexico. See att.com/dataconnectglobal for a current list of participating carriers and eligible roam zones. With respect to the countries included in the Select International Roam Zone, you will be restricted from accessing Data Service through any non-participating Canada/international wireless carriers that may otherwise be included in our generally available Canada and international wireless data roam zones. With the DataConnect North America Plan, you will be restricted from accessing Data Service through any non-participating Canada/Mexico wireless carriers that may otherwise be included in our generally available Canada and international wireless data roam zones.

DATA GLOBAL ADD-ON- May only be used with eligible Equipment. Domestic data usage not included. Qualified domestic wireless data plan required. If combined with a wireless voice plan that includes international voice roaming, your international wireless voice roaming in countries included in the Global Data Add-On's Select International Roam Zone will be limited to the participating Canada/international wireless carriers and you will be restricted from voice roaming through any non-participating Canada/international wireless carriers that may otherwise be included in our generally available Canada and international voice roam zones.

DATACONNECT GLOBAL/NORTH AMERICA PLANS - Requires minimum one-year Service Commitment and you must remain on the plan, for a minimum one-year term. Voice access is restricted and prohibited.

6.11 AT&T DataPlusSM/AT&T DataProSM Plans

6.11.1 AT&T Data Plans With Tethering

Tethering is a wireless or wired method in which your AT&T mobile device is used as a modem or router to provide a Internet Access connection to other devices, such as laptops, netbooks, tablets, smartphones, other phones, USB modems, network routers, mobile hotspots, media players, gaming consoles, and other data-capable devices. AT&T data plans with tethering enabled may be used for tethering your AT&T Mobile device to other devices. If you are on a data plan that does not include a monthly megabyte allowance and additional data usage rates, you agree that AT&T has the right to impose additional charges if you use more than 5 GB in a month; prior to the imposition of any additional charges, AT&T shall provide you with notice and you shall have the right to terminate your Service (early termination charges may apply).

6.11.2 Blackberry[®] Personal

Supports personal email access to up to 10 Internet email accounts. Users storing more than 1,000 emails or email older than 30 days, may have some emails automatically deleted. May not be used to access corporate email such as BlackBerry Enterprise Server.

6.11.3 Blackberry[®] Connect; Blackberry Enterprise; Blackberry International

Supports BlackBerry Enterprise Server[™] for corporate access (valid Client Access License required), and personal email access to up to 10 Internet email accounts as per BlackBerry Personal. BlackBerry International requires a minimum one-year agreement.

6.12 GOOD Plan

Requires compatible Good Server and, as to each end user, a compatible Good Client Access License (CAL) for use with a qualifying AT&T data plan. Solution includes software, products and related services provided by Good Technology, Inc. ("Good"), which are subject to applicable Good terms and conditions. Good is solely responsible for all statements regarding, and technical support for, its software, products and services.

6.13 Microsoft[®] Direct Push

Requires compatible Microsoft[®] Exchange Server and, as to each end user, a compatible device, a Direct Push enabled email account, and a qualifying AT&T Data Plan. Plans include end user customer support from AT&T[®] for compatible devices. AT&T does not sell, supply, install or otherwise support Microsoft[®] software, products or services (including without limitation, Exchange and Direct Push).

6.14 AT&T Mobile Share Plans (with Unlimited Talk and Text)

AT&T Mobile Share plans, including Mobile Share Value plans, allow you to share a monthly allotment of domestic wireless data usage, along with unlimited domestic talk and texting services among up to ten (10) Devices. You choose a specific allotment of monthly shared data usage for a monthly recurring charge and then pay an additional charge for each Device added to the Mobile Share plan you select. You must specifically identify the devices (the "Designated Devices") that will share your monthly allotment of data usage under the Mobile Share plan you select. If you add a WI Device for unlimited talk only, it will be counted as one of the (10) Designated Devices under the Mobile Share plan. Designated Devices can include: smartphone(s), tablet(s), gaming device(s), modem(s), netbook(s), laptop(s), mobile hotspot(s), basic or quick messaging phone(s), WI Device(s). If, during a billing period, your data usage exceeds the monthly allotment of data in the Mobile Share plan you select, plus any other data (such as available Rollover Data) that you may have for use during the billing period, you will automatically be charged for overage as specified in your rate plan. Unless specified otherwise, data allowances, including overages and Rollover Data, must be used in the billing period provided or you will forfeit that usage. Authorized users on the account may temporarily suspend data access for particular Device(s) during a specific billing cycle, but monthly charges for the suspended Device(s) will continue to apply. Tethering and/or mobile hotspot use is permitted with Mobile Share plans with capable Designated Devices; provided, however, that such use is limited to a maximum of five (5) simultaneous users per Device. An activation fee will be charged when converting from a prepaid or Session-Based plan to a Mobile Share plan or when you activate an additional Device on an existing Mobile Share plan. Access to corporate email, intranet sites and/or other business applications may be available for an additional monthly charge per Device (no additional charge for Mobile Share Value plans). Discounts otherwise applicable to your Mobile Share rate plan do not apply to the additional monthly Device charge. Additional deposits and other restrictions may apply.

®

Rollover DataSM: Only Mobile Share Value plans include the Rollover Data feature. With Rollover Data, unused data from the monthly plan allotment rounds up to the nearest MB and carries over for one billing period. **Unused Rollover Data automatically expires after one billing period or with any plan change (such as changing data amounts or termination).** Unused overage data does not roll over. Rollover Data is always consumed last, after your other data allowances. Unused Rollover Data is not redeemable for cash or credit and is not transferable including to other Mobile Share Value groups on your account. Mobile Share and Mobile Share Data-only plans do not include Rollover Data.

If you use a Mobile Share plan with any device that is not a Designated Data Device, for tethering or as a mobile hotspot with more than five (5) simultaneous users, or otherwise use the plan in any way that is inconsistent with its terms, you agree that AT&T may: (a) suspend or terminate service to the account; (b) place any non-complying Device on an appropriate Mobile Share plan; and/or (c) add any other required element of the plan.

Device upgrades: If you upgrade to a new smartphone, a discounted access charge is only available for that line when purchasing a new smartphone via AT&T NextSM or when you bring your own smartphone or you purchase a new smartphone at full retail price. If you upgrade your Device to a new smartphone on a 2-year Service Commitment, that line is ineligible for the discount and the discount is lost.

6.15 AT&T Mobile Share - Data Plans (for Data-Only Devices)

AT&T Mobile Share - Data plans allow you to share a monthly allotment of domestic wireless data usage among up to ten (10) 3G, HSPA+ or LTE Devices (excluding smartphones and basic or quick messaging phones). You choose a specific allotment of monthly shared data usage for a monthly recurring charge and then pay an additional charge for each Device added to the Mobile Share - Data plan you select. You must specifically identify one or more eligible devices (the "Designated Data Devices") that will share your monthly allotment of data usage under the Mobile Share - Data plan you select. Designated Data Devices can include: tablet(s), gaming device(s), modem(s), netbook(s), laptop(s), or mobile hotspot(s). If, during a billing period, your data usage exceeds the monthly allotment of data in the Mobile Share - Data plan you select, you will automatically be charged for overage as specified in your rate plan. If, during a billing period, you do not use all of the data allotment in the Mobile Share - Data plan you select, you will forfeit that usage. Authorized users on the account may temporarily suspend data access for particular Designated Data Device(s) during a specific billing cycle, but monthly charges for the suspended Designated Data Device(s) will continue to apply. Tethering and/or mobile hotspot use is permitted with Mobile Share - Data plans with capable Designated Data Devices; provided, however, that such use is limited to a maximum of five (5) simultaneous users per Designated Data Device. An activation fee will be charged when converting from a prepaid or Session-Based plan to a Mobile Share - Data plan or when you activate an additional Designated Data Device on an existing Mobile Share - Data plan. Designated Data Devices that are capable of accessing corporate email, intranet sites and/or other business applications may do so for no additional monthly access charge. Discounts otherwise applicable to your Mobile Share - Data rate plan do not apply to the additional monthly Device charge. Additional deposits and other restrictions may apply.

If you use a Mobile Share - Data plan with a smartphone, with any device that is not a Designated Data Device, for tethering or as a mobile hotspot with more than five (5) simultaneous users, or otherwise use the plan in any way that is inconsistent with its terms, you agree that AT&T may: (a) suspend or terminate service to the account; (b) place any non-complying Device on an appropriate Mobile Share plan; and/or (c) add any other required element of the plan.

7.0 AT&T Wireless Home Services

7.1 AT&T Wireless Home Phone Service

AT&T Wireless Home Phone ("WHP") service utilizes mobile wireless gateway Equipment now called an AT&T Wireless Internet device ("WI Device", formerly called a Wireless Home Phone device or WHP Device). With WHP service, the WI Device allows you to connect a landline phone to place and receive calls over the AT&T wireless network. See Section 3.2 for more information about how AT&T wireless service works.

WHP service provides voice service only and requires that you subscribe to an eligible wireless voice plan option, such as: (1) Wireless Home Phone unlimited plan or (2) AT&T Mobile Share plan. If your WI Device is used to roam on other carrier networks, AT&T's off-net usage restrictions apply. Text messaging, data services, features and international roaming are not supported by WHP service. If you use a wireless voice plan not designed for WHP service with your WI Device, AT&T reserves the right to switch you to an appropriate plan and bill you the associated fees for such plan.

911 calls are routed based on the wireless network's automatic location technology. You should expect to provide your location address to the emergency response center responsible for sending first responders (e.g. police, medical assistance, or fire) to your location. The WI Device has battery backup power and will work in the event of a power outage. However, if you connect a landline phone to the WI Device that itself requires external electric power to operate (e.g., a cordless phone), you will not be able to place and receive calls over that phone during a power outage.

7.2 AT&T Wireless Internet Service

AT&T Wireless Internet service (formerly Wireless Home Phone and Internet service or WHPI) also utilizes the WI Device (the WHPI service used the Home Base device. With AT&T Wireless Internet service, the WI Device allows you to connect a landline phone to place and receive calls, and to connect up to twelve (12) Internet-capable devices (one (1) via Ethernet and ten (10) via Wi-Fi) to have mobile broadband Internet access over the AT&T wireless network. See Section 3.2 for more information about how AT&T wireless service works.

AT&T Wireless Internet service requires that you subscribe to an eligible wireless voice and/or data plan to take advantage of one or both capabilities. Tiered shared data plan options allow you to share a monthly allotment of domestic wireless data usage among your connected internet-capable devices. If your data usage exceeds the monthly data allotment of the plan you select during a billing period, you automatically will be charged for overages as specified in your plan. If you do not use all of the monthly data allotment of the plan you select during a billing period, you forfeit that usage. You may also add your WI Device to your AT&T Mobile Share plan if the monthly allotment of domestic wireless data usage under your AT&T Mobile Share plan is 10 GB or more.

If your WI Device is used to roam on other carrier networks, AT&T's off-net usage restrictions apply. Messaging services and international roaming are not supported by AT&T Wireless Internet service. If you use a wireless voice and/or data plan not designed for AT&T Wireless Internet service with your WI Device, AT&T reserves the right to switch you to an appropriate plan and bill you the associated fees for such plan.

911 calls are routed based on the wireless network's automatic location technology. You should expect to provide your location address to the emergency response center responsible for sending first responders (e.g. police, medical assistance, or fire) to your location. The WI Device has battery backup power and will work in the event of a power outage. However, if you connect a landline phone to the WI Device that itself requires external electric power to operate (e.g., a cordless phone), you will not be able to place and receive calls over that phone during a power outage.

8.0 ARE THERE OTHER TERMS AND CONDITIONS THAT APPLY TO FEATURES AND APPLICATIONS?

Terms and conditions for certain features and applications are provided on the Device at the time of feature/application activation or first use. Certain features/applications will not be available in all areas at all times.

9.0 WHAT IS AT&T ROADSIDE ASSISTANCE & OPTIONAL AT&T MOBILE INSURANCE, AT&T Mobile Protection Pack & AT&T Multi-Device Protection Pack?

9.1 AT&T Roadside Assistance

AT&T Roadside Assistance ("RA") is an optional feature that may be purchased separately and automatically billed to the wireless account. RA service is provided by American Traveler Motor Club, Inc., a licensed motor club. For complete RA Terms and Conditions, refer to your RA Welcome Kit or go to att.com/roadside.

9.2 Optional AT&T Mobile Insurance, AT&T Mobile Protection Pack & AT&T Multi-Device Protection Pack

If eligible, you have 30 days from activation or upgrade to enroll in optional AT&T Mobile Insurance, AT&T Mobile Protection Pack or AT&T Multi-Device Protection Pack. For details visit www.att.com/deviceprotection. AT&T Mobile Insurance and AT&T Multi Device Insurance are underwritten by Continental Casualty Company, a CNA company (CNA) and administered by Asurion Protection Services, LLC (in California, Asurion Protection Services Insurance Agency, LLC, CA Lic. #OD63161, in Puerto Rico, Asurion Protection Services of Puerto Rico, Inc.), CNA's licensed agent for the customers of AT&T.

10.0 WHAT OTHER TERMS AND CONDITIONS APPLY TO MY WIRELESS SERVICE?

10.1 Intellectual Property

You must respect the intellectual property rights of AT&T, our third-party content providers, and any other owner of intellectual property whose protected property may appear on any website and/or dialogue box controlled by AT&T or accessed through the AT&T's websites. Except for material in the public domain, all material displayed in association with the Service is copyrighted or trademarked. Except for personal, non-commercial use, trademarked and copyrighted material may not be copied, downloaded, redistributed, modified or otherwise exploited, in whole or in part, without the permission of the owner. The RIM and BlackBerry families of related marks, images and symbols are the exclusive properties and trademarks or registered trademarks of Research In Motion Limited - used by permission. Good, the Good logo and GoodLink are trademarks of Good Technology, Inc., in the United States and/or other countries. Good Technology, Inc., and its products and services are not related to, sponsored by or affiliated with Research In Motion Limited. All other marks contained herein are the property of their respective owners.

©2012 AT&T Intellectual Property. All rights reserved. AT&T, AT&T logo and all other marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. Apple iPhone: ™ and © 2010 Apple Inc. All rights reserved. Apple is a trademark of Apple Inc., registered in the U.S. and other countries. iPhone is a trademark of Apple Inc.

10.2 Severability

If any provision of this Agreement is found to be unenforceable by a court or agency of competent jurisdiction, the remaining provisions will remain in full force and effect. The foregoing does not apply to the prohibition against class or representative actions that is part of the arbitration clause; if that prohibition is found to be unenforceable, the arbitration clause (but only the arbitration clause) shall be null and void.

10.3 Assignment; Governing Law; English Language

10.3.1 Assignment

AT&T may assign this Agreement, but you may not assign this Agreement without our prior written consent.

10.3.2 Governing Law

The law of the state of your billing address shall govern this Agreement except to the extent that such law is preempted by or inconsistent with applicable federal law. In the event of a dispute between us, the law of the state of your billing address at the time the dispute is commenced, whether in litigation or arbitration, shall govern except to the extent that such law is preempted by or inconsistent with applicable federal law.

10.3.3 English Language

The original version of this Agreement is in the English language. Any discrepancy or conflicts between the English version and any other language version will be resolved with reference to and by interpreting the English version.

10.4 Lifeline Services

As part of a federal government program, AT&T offers discounted wireless service to qualified low-income residents in selected states. For questions or to apply for Lifeline service, call 1-800-377-9450. Puerto Rico customers should contact 1-787-405-5463. For tips on how to protect against fraud, please visit the CPUC's website at, CalPhoneInfo.com.

10.5 Trial Services

Trial Services are subject to the terms and conditions of this Agreement; may have limited availability; and may be withdrawn at any time.

10.6 NOTICE REGARDING TRANSMISSION OF WIRELESS EMERGENCY ALERTS (Commercial Mobile Alert Service)

AT&T has chosen to offer wireless emergency alerts within portions of its service area, as defined by the terms and conditions of its Agreement, on wireless emergency alert capable devices.

There is no additional charge for these wireless emergency alerts. Wireless emergency alerts may not be available on all devices or in the entire service area, or if a subscriber is outside of the AT&T service area. In areas in which the emergency alerts are transmitted, such alerts may not be received by a subscriber or user of AT&T's wireless service even though the subscriber has a device capable of receiving them.

For details on the availability of this service and wireless emergency alert capable devices, please ask a sales representative, or go to att.com and click the Wireless Emergency Alerts link. This notice is required by FCC Rule 47 C.F.R. § 10.250 (Commercial Mobile Alert Service).

In transmitting emergency alerts pursuant to federal law, AT&T, including its officers, directors, employees, vendors, and agents, shall not be liable to any subscriber to, or user of, AT&T's wireless service or equipment for any act or omission related to or any harm resulting from the transmission of, or the failure to transmit, an emergency alert; or the release to a government entity or agency, public safety, fire service, law enforcement official, emergency medical service, or emergency facility of subscriber information used in connection with delivering an emergency alert.

11.0 WHAT TERMS APPLY ONLY TO SPECIFIC STATES?

11.1 California: What If There Are Unauthorized Charges Billed To My Device?

You are not liable for charges you did not authorize, but the fact that a call was placed from your Device is evidence that the call was authorized. Unauthorized charges may include calls made to or from your phone or other Device after it was lost or stolen. Once you report to us that the Device is lost or stolen and your Device is suspended, you will not be responsible for subsequent charges incurred by that Device. You can report your Device as lost or stolen and suspend Services without a charge by contacting us at the phone number listed on your bill or at wireless.att.com.

If you notify us of any charges on your bill you claim are unauthorized, we will investigate. If there are charges on your bill for calls made after the Device was lost or stolen, but before you reported it to us, notify us of the disputed charges and we will investigate. You may submit documents, statements and other information to show any charges were not authorized. We will advise you of the result of our investigation within 30 days. If you do not agree with the outcome, you may file a complaint with the California Public Utilities Commission and you may have other legal rights. While an investigation is underway, you do not have to pay any charges you dispute or associated late charges, and we will not send the disputed amount to collection or file an adverse credit report about it. While your phone is suspended you will remain responsible for complying with all other obligations under this Agreement, including but not limited to, your monthly fee. We both have a duty to act in good faith and in a reasonable and responsible manner including in connection with the loss or theft of your Device.

11.2 Connecticut: Questions About Your Service

If you have any questions or concerns about your AT&T Service, please call Customer Care at 1-800-331-0500, dial 611 from your wireless phone, or visit att.com/wireless. If you have questions about the Unlimited Local or Unlimited Long Distance Service, please call 1-800-288-2020 or visit att.com. If you are a Connecticut customer and we cannot resolve your issue, you have the option of contacting the Public Utilities Regulatory Authority (PURA). Online: ct.gov/pura; Phone: 1-800-382-4586; Mail: Connecticut DPUC, 10 Franklin Square, New Britain, CT 06051.

11.3 Puerto Rico

If you are a Puerto Rico customer and we cannot resolve your issue, you may notify the Telecommunications Regulatory Board of Puerto Rico of your grievance. Mail: 500 Ave Roberto H. Todd, (Parada 18), San Juan, Puerto Rico 00907-3941; Phone: 1-787-756-0804 or 1-866-578-5500; Online: jrtp.gobierno.pr, in addition to having available arbitration, as provided in Section 2.0.

Return to Table of Contents

V03022017

[Policy Center Home](#)

<u>ATT.NET</u>	<u>BUSINESS</u>	<u>ABOUT AT&T</u>
<u>FULL SITE</u> <u>PRIVACY</u> <u>YOUR CHOICES</u> <u>AD CHOICES</u> <u>CONTACT US</u> <u>LEGAL</u> <u>TERMS OF USE</u> © 2014 AT&T Intellectual Property. All rights reserved.		